

555-7101-307

CallPilot

Monitoring and Security for the Administrator

Product release 1.07

Standard 1.0

April 2000



How the world shares ideas.

P0905791

CallPilot

Monitoring and Security for the Administrator

Publication number:	555-7101-307
Product release:	1.07
Document release:	Standard 1.0
Date:	April 2000

Copyright © 2000 Nortel Networks, All Rights Reserved

Printed in the United States of America

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

The process of transmitting data and call messaging between the Meridian 1 and CallPilot is proprietary to Nortel Networks. Any other use of the data and the transmission process is a violation of the user license unless specifically authorized in writing by Nortel Networks prior to such use. Violations of the license by alternative usage of any portion of this process or the related hardware constitutes grounds for an immediate termination of the license and Nortel Networks reserves the right to seek all allowable remedies for such breach.

*Nortel Networks, the Nortel Networks logo, the Globemark, How the World Shares Ideas, and Unified Networks, BNR, CallPilot, DMS, DMS-100, DMS-250, DMS-MTX, DMS-SCP, DPN, Dualmode, Helmsman, IVR, MAP, Meridian, Meridian 1, Meridian Link, Meridian Mail, Norstar, SL-1, SL-100, Supernode, Symposium, Telesis, and Unity are trademarks of Nortel Networks.

MICROSOFT, MS-DOS, POWERPOINT, WINDOWS, and WINDOWS NT are trademarks of Microsoft Corporation.

PCANYWHERE is a trademark of Symantec Corporation.

SLR4, SLR5, and TANDBERG are trademarks of Tandberg Data ASA.

Publication history

April 2000

This is the Standard 1.0 issue of *Monitoring and Security for the Administrator* for CallPilot 1.07.

Contents

About this guide	15
What's new in this guide	16
Overview.	17
Skills you need	18
Multi-administrator access	19
Related information products	21
 Part 1 Maintaining the administration system	 25
 1 Getting started	 27
Overview.	28
Logging on to Windows NT on the server	29
Accessing Windows NT Administrative Tools	31
Shutting down or restarting the server	32
Creating boot disks	34
Changing the date and time	36
Viewing the server date and time from the administrative PC.	37
 2 Configuring operational measurements	 39
Overview.	40
What are operational measurements?	41
How to use OMs	43
Types of OM data	44
How Reporter uses OMs.	46
Collecting OM data.	47
 3 Adding systems and sites to the client	 49
Overview.	50
Adding a system	51
Grouping systems into a site.	54

4	Maintaining existing users	55
	Overview	57
	Section A: About managing users	59
	Basic user maintenance tasks	60
	Individual user requests	63
	Section B: Searching for users	65
	Overview	66
	What is a user search?	67
	Specifying search criteria	71
	Broadening a user search	73
	Restricting a user search	75
	Modifying and reusing your latest user search	77
	Saving a user search	78
	Running a saved user search	79
	Deleting a saved user search	80
	Section C: Managing user mailboxes	81
	Changing a user's personal information	82
	Adding/changing/canceling an administrator's access capability	83
	Temporarily preventing administrators from accessing the desktop	85
	Restoring a user's administrative desktop access	87
	Resetting a user's administrative password	89
	Changing a user's mailbox properties	90
	Deleting a user from the system	91
	Printing user account details	92
	Section D: Frequently performed tasks	93
	Reenabling a disabled mailbox	94
	Resetting a user's mailbox password	95
	Increasing a user's mailbox storage space	96
	Enabling or disabling Autologon	97
	Checking how much storage space a user has left	98
	Checking if a user has recorded greetings	99
	Checking when a user last used a mailbox	101
	Checking invalid logon attempts to a mailbox	102
5	Creating and maintaining shared distribution lists	103
	Overview	105
	Section A: About distribution lists	107
	What is a distribution list?	108
	Shared distribution lists versus personal distribution lists	110

What kinds of users can be included in shared distribution lists?	111
Guidelines for creating shared distribution lists	112
Section B: Setting up shared distribution lists	115
Opening Shared Distribution Lists	116
Setting up a shared distribution list	117
Creating and labeling the shared distribution list	119
Recording a name for the shared distribution list	120
Choosing the type of user to add to the shared distribution list	121
Using the Search Users tool to collect users for an SDL	122
Adding a single user to the shared distribution list	123
Adding all users to the shared distribution list	124
Adding a user with a known Callback DN or mailbox number	125
Creating a remote user for the shared distribution list	126
Defining the mailbox settings for a remote user	127
Recording a spoken name for a remote user	129
Importing a WAV file for the remote user's name	130
Creating a directory entry for the shared distribution list	131
Defining the settings for a directory entry	132
Recording a spoken name for a directory entry	133
Importing a WAV file for a directory entry	134
Viewing a shared distribution list	135
Viewing or changing a shared distribution list	136
Deleting a user from a shared distribution list	137
Deleting a shared distribution list	138
Printing shared distribution lists	139

6 Performing server backups 141

Overview	142
Section A: About performing server backups	143
About backing up server data	144
Section B: Working with backup devices	149
About backup devices	150
Adding backup devices to the Backup Devices window	154
Modifying or deleting backup devices	156
Section C: Scheduling server backups	159
About scheduling server backups	160
Opening the Backup Scheduler	163
Scheduling server backups	165
Modifying and deleting scheduled backups	170
Monitoring or canceling backups	171

Section D: Setting up remote disk backups	175
About remote disk backups	176
Planning the configuration	177
Creating a writable share on the remote file server	179
Reconfiguring the backup and restore on the CallPilot server	199
Verifying the network configuration	204
Creating a disk device on the CallPilot server	206
Section E: Restoring your CallPilot system	207
Restoring your CallPilot system from the base hardware.	208
7 Archiving and restoring data from archives	209
Overview	211
Section A: About archives	213
What are archives?	214
Kinds of archive	216
Why restore data from archives	217
Section B: Performing archives	219
Opening Archive Manager	220
Setting up an Application Builder archive	221
Updating an Application Builder archive	222
Removing applications from an Application Builder archive	223
Setting up a User archive	224
Updating a User archive	225
Removing users from a User archive	227
Setting up a Prompt archive	228
Setting a schedule for an archive	229
Performing an immediate archive.	231
Section C: Restoring data from archives	233
Opening Restore Manager	234
Changing the archive device.	236
Restoring Application Builder applications from an archive	237
Restoring user data	239
Selecting the languages of prompts to be restored	241

Part 2 Monitoring the CallPilot system 243

8	Introduction to monitoring CallPilot	245
	Alarms and events.	246
	Disk space usage.	249
	Server performance.	252
	Hardware problems.	253
	Reports	257
 9	 Viewing and filtering server events	 261
	About server events	262
	Using the Event Browser versus the Alarm Monitor	264
	Changing the event log size	266
	Using the Windows NT Event Viewer	269
	 Section A: Using the Event Browser	 271
	Viewing events in the Event Browser.	272
	Filtering events in the Event Browser.	275
	Saving and printing a list of events from the Event Browser	278
	 Section B: Using the Alarm Monitor	 281
	Viewing events in the Alarm Monitor	282
	Specifying when the Alarm Monitor appears in the foreground	284
	Showing the Alarm Monitor in the background.	285
	Clearing active alarms	286
	 Section C: Filtering events using the Event Preferences program	 289
	Throttling events (reducing the frequency of events).	290
	Filtering by changing event properties	292
	Adding, changing, and deleting event preferences	293
	 Section D: Configuring CallPilot to send SNMP traps to a Network Management System	 297
	Overview.	298
	Configuring SNMPs on the CallPilot server.	299
	Configuring an NMS to receive CallPilot traps	302
 10	 Viewing and filtering client PC events	 309
	Overview.	310
	Viewing client PC events	311

Filtering events in the PC Events browser	312
---	-----

11 Monitoring the server 315

Section A: Viewing switch configuration and server settings 317

About switch configuration and server settings	318
--	-----

Viewing the switch settings	319
-----------------------------------	-----

Viewing the server settings	320
-----------------------------------	-----

Section B: Monitoring disk space 323

Overview	324
----------------	-----

Monitoring Nortel directory disk space	326
--	-----

Monitoring Multimedia File System volumes	327
---	-----

General methods to monitor disk space	330
---	-----

Section C: Monitoring the database 333

Monitoring the database using alarms	334
--	-----

Section D: Monitoring server performance 337

About the Server Performance Monitor	338
--	-----

Viewing server performance data	339
---------------------------------------	-----

Printing server performance data	341
--	-----

12 Managing channels 343

Section A: Managing call channels 345

Overview	346
----------------	-----

About call channels and their states	347
--	-----

Viewing call channel states	352
-----------------------------------	-----

Starting and stopping call channels	355
---	-----

Section B: Managing multimedia channels 359

Overview	360
----------------	-----

About multimedia channels	361
---------------------------------	-----

Viewing multimedia channel states	367
---	-----

Viewing multimedia channel media types	370
--	-----

Powering multimedia channels on and off	371
---	-----

Starting and stopping multimedia channels	373
---	-----

13 Troubleshooting 377

Overview	378
----------------	-----

Section A: Outcalling services 379

Types of problems users might encounter	380
Events generated by Outcalling services	385
Using Reporter to monitor and troubleshoot Outcalling services.	388
Section B: System operation problems	391
Overview.	392
Troubleshooting checklist.	393
Troubleshooting examples	396

Part 3 Securing the CallPilot system 399

14	Introduction to CallPilot security	401
	Overview	402
	Security strategies	404
	Common hacker techniques	406
	Security threats to messaging systems	408
	How to protect CallPilot	410
15	Physically securing your equipment and data	415
	Overview	416
	Securing the premises	417
	Securing equipment	418
	Disposing of printed information	420
16	Maintaining system password security	421
	Overview	422
	Changing Nortel Networks user account passwords	423
	Changing pcANYWHERE32 passwords	429
17	Implementing CallPilot security features	431
	Overview	432
	Restrict administrators' access to the system	435
	Place dialing restrictions on features	437
	Secure users' mailboxes	439
18	Monitoring and auditing CallPilot system activity	441
	Overview	442

Section A: Reporter alerts and reports	445
What are alerts and reports?	446
Security alerts	448
Reports	451
Section B: CallPilot server tools	455
Alarms and events.	456
Server Performance Monitor	457
Windows NT Performance Monitor.	458
 19 Using Hacker Monitoring	 459
Overview.	460
Section A: About Hacker Monitoring	461
Overview.	462
Calling line ID monitoring	464
Mailbox monitoring	466
Application Builder services monitoring	468
Section B: Setting up Hacker Monitoring	471
Opening Security Administration.	472
Monitoring CLIDs for logon attempts and thru-dials.	473
Removing a CLID from the monitoring list	474
Monitoring mailboxes for logon attempts and thru-dials	475
Removing a mailbox from the monitoring list	476
Monitoring Application Builder applications for thru-dials.	477
Removing an Application Builder application from the monitoring list . . .	478
Setting up an alarm mailbox.	479
Viewing alarms.	481
 20 Security features on the Meridian 1 switch	 483
Overview.	484
Understanding dialing restrictions	487
Network Class of Service	490
Trunk Group Access Restriction and Class of Service.	494
Coordinating Meridian 1 and CallPilot dialing privileges	498
Meridian Mail Trunk Access Restriction	500
Precautions for modems	501
 Index	 503

Preface

About this guide

In this preface

What's new in this guide	16
Overview	17
Skills you need	18
Multi-administrator access	19
Related information products	21

What's new in this guide

These are the new features for CallPilot 1.07:

- You now handle maintenance, monitoring, and security tasks through two new interfaces on the administrative PC:
 - the CallPilot Administration Client Explorer, which replaces the MAT Navigator
 - the CallPilot Administration Client window, which replaces the SMI window
- There is a new Add CallPilot System wizard for connecting your clients to your servers. The Add System wizard is accessed from the new CallPilot Administration Client Explorer.
- The Backup and Restore procedure is updated for this release.
- There is a new feature that lets you configure the CallPilot server to send Simple Network Management Protocols (SNMP) traps to a Network Management System (NMS). When this service is configured you can work with server alarms on an NMS.
- There are new interfaces for managing your call channels and multimedia channels. You can monitor individual call channels through the Channel Monitor and individual multimedia channels through the Multimedia Monitor.

Overview

Introduction

Monitoring and Security for the Administrator provides the information and instructions required to maintain a CallPilot system, and to troubleshoot any problems that arise.

For information on how to replace a CallPilot server hardware component, refer to the installation guide appropriate to your server type.

Who should read this guide

This guide is developed for system administrators who are responsible for the maintenance, monitoring, and security of the CallPilot system.

Monitoring tools available to you

There are many ways that you can monitor the system:

- Use Reporter to monitor traffic and usage patterns and system resource usage.
- Use CallPilot tools to monitor hardware component problems, CPU, disk space, and server performance levels.
- Use Windows NT server tools.
- Use SNMP traps to work with server alarms on an NMS.

Security tools available to you

There are a number of security tools that you can use to make your system safe:

- monitoring and auditing system activity using alarms and reports
- securing your equipment and data
- securing users' mailboxes
- using Hacker Monitoring

Skills you need

Switch technology knowledge

Knowledge of, or experience with, one or more of the following products is recommended:

- Meridian 1 PBX equipment, X11 release 23c and greater
- SL-100
- Lucent equipment
- Mitel equipment
- Rolm equipment
- Matra equipment

PC experience or knowledge

Knowledge of, or experience with, the following PC products is of assistance:

- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT
- Microsoft Windows 2000 Professional
- pcANYWHERE32
- TCP/IP protocols

Other experience or knowledge

Other types of experience or knowledge that might be of use include the following:

- network management
- client-server systems
- flowcharting
- troubleshooting

Multi-administrator access

Introduction

You can create multiple administrator accounts to make administering CallPilot easier and more efficient. Multiple accounts enable administration responsibilities to be distributed among a number of people. Therefore, certain administrators can specialize in certain tasks, such as maintaining users, performing backups, analyzing reports, or creating multimedia services.

For more detailed information, see the *Administrator's Guide*.

Access classes

For security reasons, administrators should be given access only to those parts of the system that relate to their role. For example, an administrator who is responsible only for creating multimedia services should have access only to Application Builder and the Service Directory Number Table.

Each administrator account is assigned an access class. An access class is a list of system parts and the level of access allowed for each part. The access levels are

- create/delete (enables an administrator to delete objects such as users and services)
- edit
- create/delete/edit
- view
- none

For example, an administrator might be able to create or delete objects in Application Builder but only view User Templates.

Simultaneous access

Multiple administrators can log on to CallPilot at the same time without overwriting other work.

If you are the first to log on to a particular resource, such as a specific mailbox class or user profile, and another administrator tries to access the same resource, a dialog box appears to inform you of the other administrator. At this point, you can do one of the following actions:

- Keep editing.
- Save your changes, and release the resource to the other administrator.
- Cancel your changes, and release the resource to the other administrator.

If you do not respond to this prompt within two minutes—because you are away from the terminal, for example—the system releases the resource so that others can access it. If this happens, all your unsaved changes are lost.

An administrator who accesses a resource that is currently being edited sees a read-only view of the property sheet in which all boxes are dimmed. This indicates that the resource is currently locked. The administrator is not notified when the resource is released, but must try to access the property sheet again to see whether its status has changed.

If a user tries to log on to a mailbox while an administrator is changing the profile, the user is unable to log on and receives a message that says the mailbox is in use.

Refreshing screens

Because multiple administrators can access the same database at the same time, a Refresh command is available from the View menu to ensure that the view you are seeing is the most recent.

For example, if you are viewing a list of users when another administrator deletes a user, the only way to see the change is to refresh the screen. Therefore, refresh the screen regularly.

Related information products

Introduction

The following list of CallPilot technical documents are stored on the CD-ROM that you receive with your system. You can search the entire suite of documentation online, or you can print part or all of a guide.

Planning and engineering guides

Use these guides before you install CallPilot to help plan your system, and to plan a migration of data from Meridian Mail to CallPilot.

Document Title

Planning and Engineering Guide

Meridian Mail to CallPilot Migration Utility Guide

Installation and configuration guides

These guides describe how to install hardware and software for the CallPilot server, client, and desktop messaging. Instructions for configuring the switch are also provided.

Document Title

200i Installation and Configuration Guide

702t Installation and Configuration Guide

1001rp Installation and Configuration Guide

Desktop Messaging Software Installation and Maintenance Guide

Administration guides

These guides provide specialized information to help you configure CallPilot, administer and maintain it, and use its features.

Document Title

Getting Started Quick Reference Card

Administrator's Guide

Reporter Guide

Application Builder Guide

Monitoring and Security for the Administrator

Networking guides

These guides describe how to plan, install, set up, and troubleshoot networking services.

Document Title

Network Planning Guide

AMIS Implementation and Administration Guide

Integrated AMIS Implementation and Administration Guide

NMS Implementation and Administration Guide

Enterprise Implementation and Administration Guide

VPIM Implementation and Administration Guide

End user guides

These guides are intended for end users of CallPilot, such as phoneset users and desktop messaging users.

Document Title

Multimedia Messaging User Guide

Speech Activated Messaging User Guide

Desktop Messaging Quick Reference Guide

Trouble-shooting reference

This reference provides step-by-step troubleshooting procedures for CallPilot.

Document Title

CallPilot Troubleshooting Reference

Using the online Help, guides, and tutorials

CallPilot contains three online sources for information:

- Online Help provides brief answers to the questions “What’s this?” and “How do I...?”
- Online guides provide detailed conceptual information, as well as information on how to perform detailed tasks.
- Online tutorials provide a complete product overview, as well as specific information on how to use Application Builder.

You can access all information using either the Help menu or Help buttons.

Contacting Technical Support

Contact your distributor’s technical support organization to get help with troubleshooting your system.

Contacting Nortel Networks

If you have comments or suggestions for improving CallPilot and its documentation, contact Nortel Networks at the following web site address:

http://www.nortelnetworks.com/callpilot_feedback

Part 1

Maintaining the administration system

In this part

Chapter 1: Getting started	27
Chapter 2: Configuring operational measurements	39
Chapter 3: Adding systems and sites to the client	49
Chapter 4: Maintaining existing users	55
Chapter 5: Creating and maintaining shared distribution lists	103
Chapter 6: Performing server backups	141
Chapter 7: Archiving and restoring data from archives	209

Chapter 1

Getting started

In this chapter

<u>Overview</u>	<u>28</u>
<u>Logging on to Windows NT on the server</u>	<u>29</u>
<u>Accessing Windows NT Administrative Tools</u>	<u>31</u>
<u>Shutting down or restarting the server</u>	<u>32</u>
<u>Creating boot disks</u>	<u>34</u>
<u>Changing the date and time</u>	<u>36</u>
<u>Viewing the server date and time from the administrative PC</u>	<u>37</u>

Overview

Introduction

This chapter provides general CallPilot procedures that you should be familiar with before you begin server software maintenance.

Logging on to Windows NT on the server

Introduction

When logging on to Windows NT on the server, ensure that the CAPS key is not on. The password is case-sensitive.

Follow the procedure in this section to log on to Windows NT with administrator privileges.

To log on as Administrator

- 1 Start the server. The Windows NT logon prompt appears.



- 2 Press Ctrl+Alt+Del.

Result: The logon dialog box appears.



- 3 Type **Administrator** as the user ID.
- 4 Type the password.

Note: The default password is abc123, but the installer is instructed to change this password during the server installation on-site, so a new

password should be in place at this point. If you do not know the password, check with the administrator.

- 5 Click OK.

Result: The Windows NT desktop appears.

Accessing Windows NT Administrative Tools

To access a Windows NT administrative tool

- 1 Log on to the server as Administrator.
- 2 Choose Start > Programs > Administrative Tools (Common), and select the tool you want to run.

List of Administrative Tools

The following are among the tools available from the Windows NT Administrative Tools menu:

- Backup
- Disk Administrator
- Event Viewer
- Performance Monitor
- User Profile Editor
- User Manager
- Server Manager
- Windows NT Diagnostics

For more information, consult your Windows NT documentation.

Shutting down or restarting the server

Introduction

Follow the procedures in this section to shut down the CallPilot server properly.



CAUTION

Risk of file corruption

Do not press the power button on the front of the server to shut down your system. This can result in file corruption. If possible, perform the system shutdown described in this section instead.

To shut down or restart the CallPilot server

- 1 Click Start > Shutdown.

Result: The Shut Down Windows dialog box appears.



- 2 If you need to turn off the server, select Shut down. If you want to restart the server, select Restart. Then click Yes.

Result: You might be informed that an SQLAnywhere service is running with connections, and asked if you want to end it.

- 3 Click Yes.

Result: You might also be asked if you want to save ACD proxy changes.

4 Click No.

Result: If you are shutting down the server, the CallPilot server shuts down and powers off. If you are restarting the server, it shuts down and then begins starting up.

5 If you are going to work on the inside of the server, follow proper safety precautions as described in the *Installation and Configuration Guide* for your hardware platform.

Creating boot disks

Introduction

If the system does not start from the hard disk, you need to start it from a boot disk. Follow the procedures in this section to make any disk bootable.

Choosing a procedure

If you have access to a computer that is running properly, use the first procedure in this section. If not, create a boot disk by following the second procedure.

To create a boot disk using the hard disk

- 1 Start MS-DOS.
- 2 Insert the disk that you want to make bootable into the disk drive (drive A).
- 3 Type **sys a:** and press Enter.
- 4 Type **copy c:\dos\himem.sys a:** and press Enter.
- 5 Create a config.sys file on the disk that contains the following lines:

```
device=himem.sys
```

```
dos=high
```

Note: Refer to MS-DOS documentation for more information on creating boot floppies.

To create a boot disk using the MS-DOS disk

Note: Use this procedure if you do not have access to a PC that is running properly. For this procedure, you are asked to switch the disks between disk drives A and B. Disk drives A and B are the same drive. Therefore, you have to switch the disks for this one drive.

- 1 Insert the MS-DOS installation disk into the disk drive, and restart the system.

Result: The MS-DOS Setup screen appears.

- 2 Press F3 twice to exit.
Result: The system displays the a:\ prompt.
- 3 Type **sys b:**
Result: The system asks you to insert a disk into drive B.
- 4 Place the target disk in the disk drive and press Enter.
Result: The system asks you to insert a disk into drive A.
- 5 Remove the target disk from the disk drive.
- 6 Place the source disk back into the disk drive and press Enter.
Result: The system asks you to insert a disk into drive B.
- 7 Reinsert the target disk into the disk drive and press Enter.
- 8 Continue to remove and insert the target and source disks as prompted until the following message appears: `System transferred.`
- 9 Reinsert the source disk and press Enter.
Result: The system returns to the a:\ prompt.
- 10 Type **expand himem.sys_ b:\himem.sys**
- 11 Reinsert the target disk.
Result: The system responds with this message:
`himem.sy_ --> b:\himem.sys`
- 12 Insert the source disk and press Enter.
Result: The system responds with this message:
`1 file expanded.`
- 13 Once the system returns to the a:\ prompt, restart the computer. If you want to test the boot disk, restart the computer with the target disk in the disk drive.

Changing the date and time

Introduction

The CallPilot server makes adjustments in the date and time to stay synchronized with the Meridian 1 switch. If you attempt to change the date and time on the server, the server automatically readjusts the time to stay synchronized with the M1 switch. To achieve a proper time change, the switch administrator must change the date and time at the switch.

Note: For the server's capability to synchronize date and time with non-M1 switches, refer to documentation for your specific switch.

Example: Change from daylight saving time to standard time

During a time change from daylight saving time to standard time, the following events occur:

- Windows NT on the server automatically adjusts the time.
- Within ten minutes, the server changes the time back to ensure that it is synchronized with the Meridian 1 switch time.

Note: Some system components might be restarted automatically to recover from the automatic time change.

Viewing the server date and time from the administrative PC

Introduction

The system time is shown in a box in the bottom right corner of the CallPilot Administration Client window on the administrative PC.

To view the system date, time, and time zone

- 1 Select Start > Programs > Nortel Networks CallPilot Administration Client.

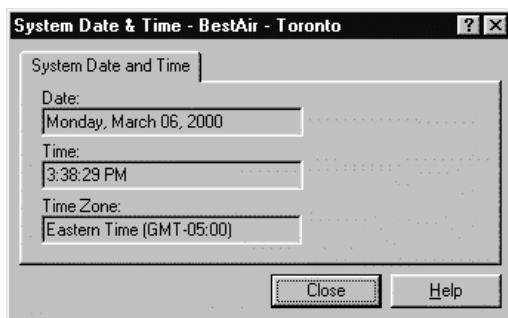
Result: The CallPilot Administration Client Explorer appears.

- 2 Double-click a system and log on.

Result: The CallPilot Administration Client appears.

- 3 From the CallPilot Administration Client window, double-click the time located at the bottom right corner of the window.

Result: The System Date & Time property page appears.



- 4 Click Close to return to the CallPilot Administration Client window.

Chapter 2

Configuring operational measurements

In this chapter

Overview	40
What are operational measurements?	41
How to use OMs	43
Types of OM data	44
How Reporter uses OMs	46
Collecting OM data	47

Overview

Introduction

This chapter explains operational measurements and how you can collect and interpret them to improve system performance.

What are operational measurements?

Introduction

Operational measurements (OMs) are statistics that provide valuable information about the way your CallPilot system is used. Some OMs provide detailed information about phone calls processed by the system. Other OMs provide general information about system resources, such as disk space and channel usage.

Programs and tools such as Reporter use OMs to help improve CallPilot system efficiency. Use the data OMs provide to help you

- monitor system performance
- improve system security
- track message delivery
- troubleshoot hardware and software problems

Programs and tools that use OMs

The following programs and tools use OMs:

Program or tool	Description
Reporter	<p>Generates reports based on raw OM data.</p> <p>Generates alerts warning users of hardware or software problems.</p> <p>Uses Audit Trail to provide detailed information about message delivery to external users. The audit trail includes Remote Notification (RN) messages, Delivery to Telephone (DTT) messages, and Delivery to Fax (DTF) messages. You can determine whether the system tried and failed to deliver messages.</p> <p>Can summarize the information collected by Hacker Monitoring and Session Trace.</p>

Program or tool	Description
Hacker Monitoring	Allows you to track suspicious activities on mailboxes or specific telephone numbers.
Session Trace	Gathers basic information for each call session of a mailbox. You can troubleshoot why messages were lost, delayed, or not delivered.

How to use OMs

Introduction

Before CallPilot programs or tools can use OM data, you must configure the CallPilot server to collect and store OM data.

Collect and store OM data

To collect OM data from the server, you must specify

- the type of data you want to collect
- the interval at which data will be collected
- the length of time data will be stored on the server

Specify the type of OM data

The CallPilot server can collect three types of OM data: trace, billing, and traffic. Each type of data provides different information on how your system is used.

For more information, see [“Types of OM data” on page 44](#).

Specify the interval for data collection

The CallPilot server can collect OM data 24 hours a day, or once a day during a specified period. You might want to collect OMs 24 hours a day if your company receives faxes or phone calls from international locations, or if you are concerned about hacker activities during nonbusiness hours.

If you do not want to collect OMs 24 hours a day, you must decide on an appropriate interval for data collection. If your business is open from 9:00 a.m. to 5:00 p.m., for example, you might want to collect OM data only during those hours.

Specify how long OMs are stored on the server

The CallPilot server automatically stores OM data for seven days. If you want to keep data on the server for a different length of time, you can specify a storage period of one to ten days.

Types of OM data

Introduction

The CallPilot server can collect three types of OM data:

- Billing
- Traffic
- Trace

Each type of data provides different information on how your system is being used.

Billing OMs

Billing OMs provide information about each phone call handled by your CallPilot system. When a call is processed, billing OMs record the

- name of the service the user accessed
- number the user dialed
- duration of the call
- number of logon attempts

Reports generated from billing OMs can help ensure that company expenses are allocated correctly. For example, you can use billing OMs to determine which users have made long distance phone calls. Then you can bill either the user or the user's department for the expense.

Note: If you set your server to collect billing OMs, it automatically collects traffic OMs as well.

Traffic OMs

Traffic OMs provide information about how CallPilot services are being used. Unlike billing OMs, which record detailed information about every call handled by the system, traffic OMs summarize information related to calling activity. This information includes

- how many incoming and outgoing calls the system processes
- how often services such as networking and outcalling are accessed

Reports generated from traffic OMs can help you to assess the overall efficiency of your system. For example, if traffic OMs indicate that channels 1 and 2 handled 100 calls in an hour, but channel 3 did not handle any, channel 3 might have failed and needs to be replaced.

Trace OMs

Trace OMs provide information about the Speech Activated Messaging service (SAM). Trace OMs record information such as

- the caller DN
- the mailbox
- the total number of successful logon attempts

The information provided by trace OMs is specialized and is used to generate only one report. The SAM report can help you to assess the overall efficiency of your SAM service. For example, if trace OMs indicate that there is a low number of successful logon attempts you can give users additional training on SAM.

Note: If you set your server to collect trace OMs, it automatically collects traffic and billing OMs as well.

How Reporter uses OMs

Introduction

Reporter converts the OMs collected by your CallPilot server into easy-to-read reports. These reports can help you to

- establish a pattern of normal system behavior
- monitor system usage
- monitor system security
- detect potential system problems
- assess your system's overall efficiency
- bill users for service usage
- track administrator-level actions
- predict future resource requirements

For detailed information about how different types of OM data determine what kinds of reports you can generate, see the *Reporter Guide*.

For more information on how OM data and reports are used in the monitoring of your system, see [“Reports” on page 257](#).

Collecting OM data

Introduction

Before the server can start gathering OM data, you must specify the type of data you want to collect, the interval at which the data will be collected, and the length of time the data will be stored on the server.

Note: By default, the server collects Billing OMs 24 hours a day and stores this data for seven days.

Type of data

The type of OM data you collect determines which reports you can generate.

If you do not want your server to collect OM data, you can specify None when setting your collection parameters. This prevents OMs from taking up valuable space on the server. Choose None only if you do not want to generate reports.

Data storage

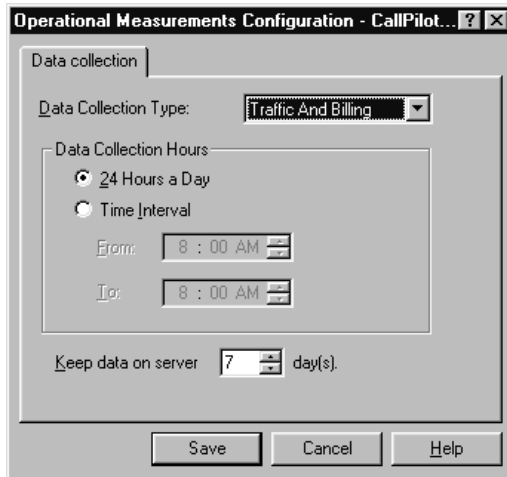
The server automatically stores OM data for seven days. If you want to keep data for a different length of time, specify a storage period of one to ten days.

Note: Storing OM data affects the amount of disk space available on your server. If your free disk space is below 20 percent, storing OMs for ten days can reduce server performance. You might notice a slow response from the server or, if too much disk space is used, an alarm might be generated.

Getting there CallPilot System > System Administration > System Performance Monitoring > Operational Measurements

To collect OMs

- 1 From the Data Collection Type list, select the type of data you want to collect.



- 2 If you want to collect data 24 hours a day, click 24 Hours a Day.
 - 3 If you want to collect data for part of the day, click Time Interval. Then, in the From box, select the start time for data collection. In the To box, select the end time for data collection.
 - 4 In the Keep data on server box, select the number of days for which data is stored, or accept the default.
- Note:** You can store data for one to ten days.
- 5 Click Save to return to the CallPilot Administration Client window.

Chapter 3

Adding systems and sites to the client

In this chapter

Overview	50
Adding a system	51
Grouping systems into a site	54

Overview

Introduction

This chapter describes how to add a system to CallPilot, and how to group your systems into sites.

Adding a system

Introduction

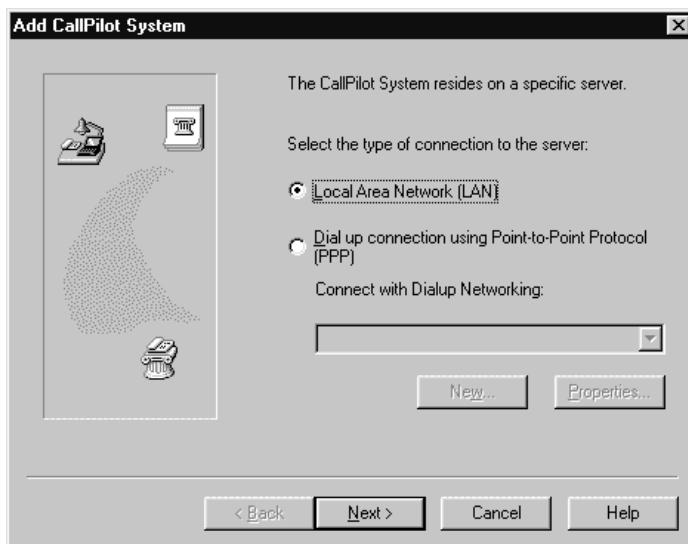
Use the Add CallPilot System wizard to add a system to the site.

Getting there Start > Programs > Nortel Networks CallPilot Administration Client

To add a system to the site

- 1 Double-click Add System.

Result: The first screen of the Add CallPilot System wizard appears.



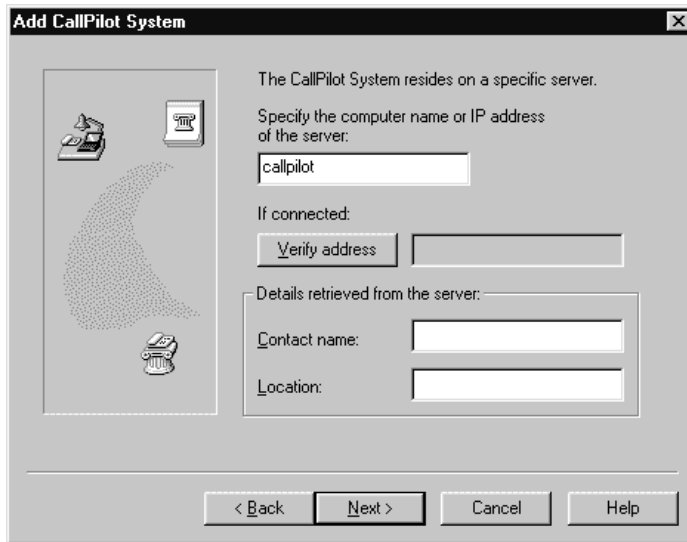
- 2 A system resides on a specific server. Select the type of connection to the server (Local Area Network or Dial up connection).

If the administrative PC is on the same local network as the server, choose Local Area Network (LAN); otherwise, choose Dial up connection.

Note: For instructions on configuring a dial-up connection, refer to the Windows operating system documentation. When the dial-up connection is configured, continue with the next step in this procedure.

3 Click Next.

Result: The second screen of the Add CallPilot System wizard appears.



4 Enter the computer name or the Customer LAN (CLAN) IP address of the server that you want to add to CallPilot.

Note: If, at this point, you are not connected to any servers, CallPilot will locate the server when you connect at a future time.

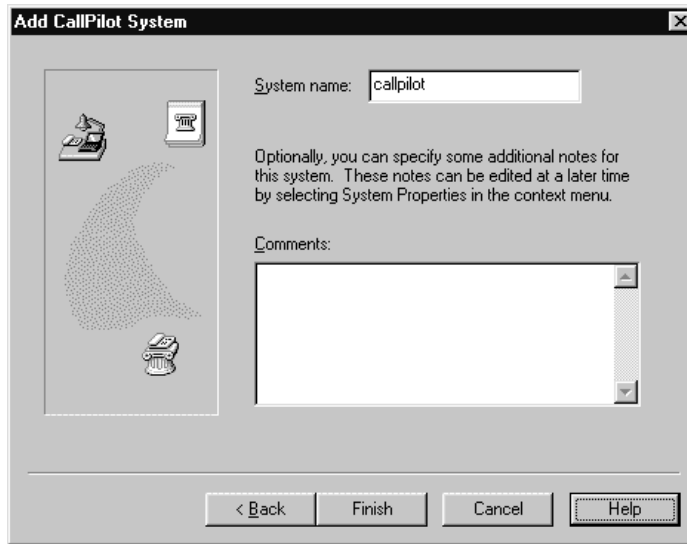
5 Click Verify Address to verify that the administrative PC can connect to the server.

If you use the computer name to identify the server, then this step inserts the CLAN IP address for the server. Also, if the server has a Contact Name and Location defined, this information is inserted into the Add System wizard.

Note: This step tests your connection to the server (system). If you get an error message, make sure that your IP address or computer name is correct. If you are not connected to the server or the server is offline, when you click Verify address you get an error message. However, CallPilot finds the server when you connect the client to the server at a future time.

- 6 Click Next.

Result: The last screen of the Add CallPilot System wizard appears.



- 7 If necessary, change the name of the system. The system name must follow standard Windows operating system file naming rules (for example, no symbols).

In Comments, enter any notes or comments about the system that you require.

- 8 Click Finish.

Result: The system name is displayed in the right pane of the CallPilot Administration Client Explorer.

Grouping systems into a site

Introduction

You can group systems logically by placing them into folders with meaningful names.

The site folders appear in the left pane of the CallPilot Administration Client Explorer window.

To group systems into a site

- 1 Create a subfolder in the CallPilot Administration Client Explorer folder.
- 2 Name the subfolder with the site name.
- 3 Click and drag the systems into the new site folder.

Chapter 4

Maintaining existing users

In this chapter

Overview	57
Section A: About managing users	59
Basic user maintenance tasks	60
Individual user requests	63
Section B: Searching for users	65
Overview	66
What is a user search?	67
Specifying search criteria	71
Broadening a user search	73
Restricting a user search	75
Modifying and reusing your latest user search	77
Saving a user search	78
Running a saved user search	79
Deleting a saved user search	80
Section C: Managing user mailboxes	81
Changing a user's personal information	82
Adding/changing/canceling an administrator's access capability	83
Temporarily preventing administrators from accessing the desktop	85
Restoring a user's administrative desktop access	87
Resetting a user's administrative password	89
Changing a user's mailbox properties	90
Deleting a user from the system	91

<u>Printing user account details</u>	<u>92</u>
<u>Section D: Frequently performed tasks</u>	<u>93</u>
<u>Reenabling a disabled mailbox</u>	<u>94</u>
<u>Resetting a user's mailbox password</u>	<u>95</u>
<u>Increasing a user's mailbox storage space</u>	<u>96</u>
<u>Enabling or disabling Autologon</u>	<u>97</u>
<u>Checking how much storage space a user has left</u>	<u>98</u>
<u>Checking if a user has recorded greetings</u>	<u>99</u>
<u>Checking when a user last used a mailbox</u>	<u>101</u>
<u>Checking invalid logon attempts to a mailbox</u>	<u>102</u>

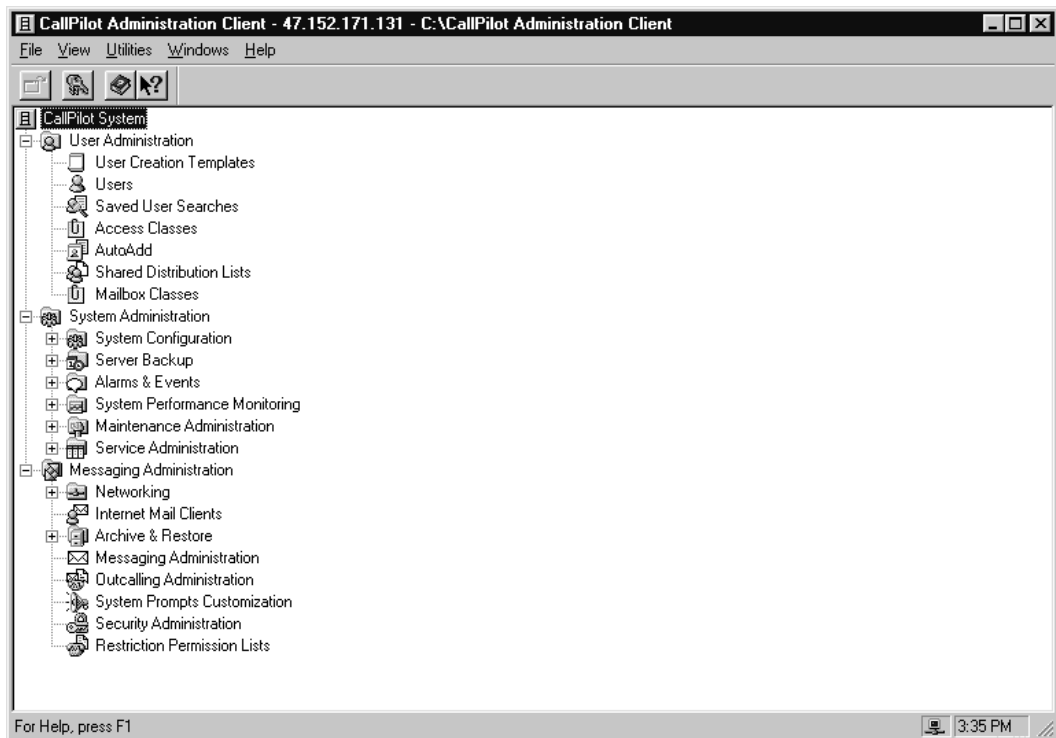
Overview

Introduction

This chapter provides information and procedures for the common tasks that maintain users on the system. Once you have added users to the system, you might need to search for them, change their properties, print details, or delete those users who have left your company.

This chapter also covers the tasks necessary to maintain and update your configured system. The tasks include performing regular administrative tasks and monitoring mailboxes.

You access your administrative tasks from the CallPilot Administration Client as shown below:



Section A: About managing users

In this section

Basic user maintenance tasks	60
Individual user requests	63

Basic user maintenance tasks

Introduction

With the Users program, you can

- search through the list of currently defined users; sorting and filtering the list to create subsets of the list
- delete users from the system
- modify the details that define a user's access attributes
- view and manage user's mailbox capabilities

Note: You can also add users to the system using the User Creation Templates.

Getting there CallPilot System > User Administration > Users

The Users dialog box

The Users dialog box appears.

Last Name	First Name	Mailbox number	Callback DN	Mailbox class	User type	Volume ID
Ackers	Deb	2211	63432211		Temporary Remote...	1
admin	admin					0
Akai	Darren	7520	7520	20m5d	Local User	1
Akai	Darren					0
ALDERMAN	LORA	2146844295	612146844295		Temporary Remote...	1
Aleong	David	7718	7718	20m5d	Local User	1
Algonquin			7203		Directory Entry User	1
ALLEN	SAMUEL	5230	5230		Temporary Remote...	1
Allen	Kurt					0
ALLISON	DALE	2414	66552414		Temporary Remote...	1
Alvarez	David	4440487	64440487		Permanent Remote...	1
ADYAMA	AMY	2595	66552595		Temporary Remote...	1
Archibald	Ron	3770	63433770		Temporary Remote...	1
ASHBY	LYNN	4456403	64456403		Temporary Remote...	1
Ather	Adel	7870	7870	20m5d	Local User	1
Audio Lab	Audio Lab	7515	7515	20m5d	Local User	1
Avery	Erik	36304	36304		Temporary Remote...	1
Baetoniui	Catalin	7679	7679	20m5d	Local User	1
Baetoniui	Catalin					0
Baetoniui	Catalin					0
BAHALL	RISHI	7732	7732	20m5d	Local User	1

Note: For the sake of simplicity, a step is skipped here. The Users window displays a list of users only if you first conduct a search for users. The list of users that appears in the Users window is the result of such a search. For information on how to perform a search, see [Section B: “Searching for users.” on page 65](#).

Information associated with a user

User information is divided into

- general information
- administrative capabilities
- messaging capabilities

When you view a list of users in the Users window or a user's details in the User property sheet, you can toggle between views to see both types of information. To open the User Properties window in addition to the Users window, either right-click the desired user's name and then click Properties on the pop-up menu, or select the user and then click the Properties icon on the Users window toolbar.

General information

General information refers to a user's personal information: first name, last name, title, department, and comments about the user.

Administrative capabilities

Administrative capabilities refer to the access a user has to system administration functions. Most users do not require administrative capabilities. Those who do can have different access to the various programs in CallPilot, depending on the tasks they need to perform. For each program, an administrative user can have Create/Edit/Delete privileges, Create/Delete privileges, Edit privileges, View only privileges, or no privileges. This configuration of privileges is determined by the settings in the administrative user's access class.

Most users should not have administrative access unless they have a job responsibility to directly maintain the system.

Messaging capabilities

Mailbox capabilities refer to a user's mailbox and its associated messaging capabilities. You can change almost all of the options for an individual user who has mailbox capabilities, including the mailbox number and mailbox greetings.

Example of common changes to a user

If a user within your company moves to another job, takes on new tasks, or transfers to a new department, you might want to update his or her general information, administrative capabilities, and mailbox capabilities.

Similarly, if the role of an entire group of users changes (for example, all senior managers receive full system access), you might need to update their administrative capabilities. Likewise, policy changes or abuse of the outcalling feature might require changing the abilities of an entire mailbox class.

Individual user requests

Introduction

Administrators are often asked to change or enhance a user's mailbox capabilities, or to help users who are having problems or have been locked out of their mailboxes.

Types of user problems

Common user problems include

- forgotten passwords
- expired passwords
- mailbox lockout after too many failed logon attempts
- preference that the administrator configure certain features that can be configured through the phoneset interface on the user's phone

Types of requested enhancements

Common mailbox enhancement requests include

- increased mailbox storage capacity
- Remote Notification capacity
- assignment to a mailbox class with greater messaging options

Where to find common tasks

Look at [Section C: “Managing user mailboxes,” on page 81](#) and [Section D: “Frequently performed tasks,” on page 93](#). They provide specific tasks to resolve the types of problems mentioned above.

Check user status

You often need to check aspects of a user's status, including the number of failed logon attempts to check for possible hacker attack, or the amount of remaining storage space in the user's mailbox.

See “Setting up mailbox security” in the *Administrator's Guide* for more information on how to monitor mailboxes that you suspect are being hacked.

Section B: Searching for users

In this section

Overview	66
What is a user search?	67
Specifying search criteria	71
Broadening a user search	73
Restricting a user search	75
Modifying and reusing your latest user search	77
Saving a user search	78
Running a saved user search	79
Deleting a saved user search	80

Overview

Introduction

To change any aspect of a user account, you first need to search for and find the user:

- how to search for users

Start from a list of all users on your system. Reduce the list to a manageable size by filtering out unwanted records, then sort the rest. You end up with a sublist that contains only those records that are similar (and ordered) in a way that meets your needs. Use the Search Users function to create this sublist.

- when to search for users

Every time you use the Search Users function, you either conduct a search or call up a previously saved search.

Once you have isolated the user or group of users you need, you can perform any number of maintenance tasks.

- Search Users dialog box

The Search Users dialog box automatically appears when you start the Users program. Double-click the Users icon in the CallPilot System program tree.

What is a user search?

Introduction

A user search is something you can perform. It is also something you can create, save, and delete to save time in subsequent searches:

- something you perform
Perform a user search by first supplying the user search function with a set of conditions (using the Search Users dialog box), then activating the function.
- something you create, save, and delete
A user search is the set of conditions the search function processes to produce a sublist. You give a search a name that reflects the characteristics of the sublist the program generates.
- define the search conditions
Set search conditions by specifying three pieces of information:
 - the user field on which to base the search (for example, First Name)
 - the value to search for (for example, Marc)
 - a logical statement connecting the two. For example, connect them as equals or not equals (Is, or Is Not)
 - Example: First Name - Is - Marc

Search Criteria

The Search Criteria field is common to all user records. A search through user records examines only the contents of the chosen field(s) for each user. The list of possible criteria is provided with the search function.

Search Users - Untitled

Search for users that meet: ☒ All conditions ☐ At least one condition

Conditions

	Search Criteria	Operator	Value
1	Last Name	is	*
2	(None)		
3			

Select View: Messaging Users

Buttons: Search Now, Clear Search, Cancel, Help

Note: Based on the programs installed on your system, additional search criteria might be available.

For a list of all the possible searchable fields in CallPilot, see the “Available search criteria” in the online Help.

Value

The field Value refers to the contents of the Search Criteria field. For example, if you are interested in all users with the last name Smith, then the Search criteria is Last Name and the Value statement is Smith.

Alphanumeric criteria require alphanumeric values. Numeric criteria require numeric values.

Note: The Value statement is not case-sensitive.

Wildcards

The term “wildcard” refers to a special character that represents a string of any characters. The CallPilot wildcard character is the asterisk (*). If you include an asterisk in your value statement, the search function might find many more matching records than without the asterisk.

Use wildcards in the value statement when your search requirements are more general. For example, if you are interested in all users with last names beginning with the letter S, select Last Name from the Search Criteria list and type S* in the Value box.

Use wildcards in the value statement when you are searching for user last names you are not sure how to spell. Your value statement should contain as much of the last name as you know, with an asterisk to represent the part you are unsure of. For example, if you know the user's last name begins with Sm, then type Sm* in the value box. The search produces a sublist of users with last names that begin with Sm (for example, Smilla, Smith, Smothers, Smythe).

Placeholder

A placeholder is a special character that represents any single character. The CallPilot placeholder character is the question mark (?). If you include a question mark in your value statement, the search function might find more matching records than without the question mark. For example, if you type "J??n" in the value box with the search criteria set to First Name, the search produces a sublist of users with the first names John and Joan. However, it does not include Johann, because this name has too many letters.

Operator

The Operator specifies the relationship linking the Search Criteria field and Value statement. Records that meet the value of the criterion are either selected or ignored, based on the operator.

Four possible operators can be used in a user search when the criterion and value are numeric:

- is (=)
- is not (<>)
- greater than (>)
- less than (<)

Two possible operators can be used in a user search when the criterion and value are alphanumeric:

- Is

- Is Not

Common user searches

The following are examples of common searches:

Search criteria	Result
Last Name is Smith	Retrieves a sublist of all users named Smith
Last Name is Sm*	Retrieves a sublist of all users with last names beginning with Sm
Title is Manager	Retrieves a sublist of all users who are managers
Title is NOT Manager	Retrieves a sublist of all users who are not managers
Department is Human Resources	Retrieves a sublist of all users who are members of the Human Resources department
Invalid logon attempts greater than 1	Retrieves a sublist of all users who entered an incorrect user ID and password more than once

See also

- [“Overview” on page 66.](#)
- [“Specifying search criteria” on page 71.](#)
- For a list of all the possible search criteria, see “Available search criteria” in the online Help.

Specifying search criteria

Introduction

You can search for a user by using most fields in the user templates.

Getting there CallPilot System > User Administration > Users

To retrieve a list of all users in the system

- 1 Do not change the default settings in the Search Users dialog box.
- 2 Click Search Now.

To perform a specific search

- 1 Beside Search for users that meet, click a button to choose the type of search.
 - All conditions means that only users who meet all the conditions set in your search will be included in the search results.
 - At least one condition means that a user only needs to meet one of the conditions set in your search to be included in the search results.
- 2 From the Search Criteria list, select the search criteria.
- 3 From the Operator list, select an appropriate operator.
- 4 From the Values list, enter or select an appropriate value.

Note: Depending on the search criteria you select, you can enter a value in the Value box or select from a list of values generated by the Value box.

- 5 From the Select View list, select an appropriate view.

Note: The view determines how users are presented when a user search is completed. The General view shows general information about the user (for example, his or her title, department, and name). The Administrative view shows the user's administrative capabilities (for example, his or her password retry count and access class). The Messaging view shows the user's mailbox capabilities (for example, mailbox class or the Target Number for a paging device).

6 Click Search Now.

Result: The Users window appears, showing the results of the user search.

See also

- [“Broadening a user search” on page 73.](#)
- [“Restricting a user search” on page 75.](#)
- For a list of all the possible search criteria, see “Available search criteria” in the online Help.

Broadening a user search

Introduction

If you cannot find the user(s) you are looking for, you can widen the scope of your search. A wider search increases the number of matches your search produces.

Example

In your system, some users are Shift Managers while others are Department Managers. You know that your target user is one or the other.

To view a list that contains both types of managers, search for User Title = Shift Manager OR User Title = Department Manager.

Before you begin

You must have already specified at least one set of search conditions and run one search. If you have not, see [“Specifying search criteria,” on page 71.](#)

Getting there CallPilot System > User Administration > Users

To perform a broadened user search

- 1 Click At least one condition. This means that a user only needs to meet one of the conditions set in your search to be included in the search results.
- 2 From the Search Criteria list in the Condition2 row, select the additional criteria with which you want to search.
- 3 From the Operator list in the Condition2 row, select an appropriate operator.
- 4 In the Value list in the Condition2 row, type an appropriate value.
- 5 If desired, fill in the Search Criteria, Operator, and Value to add a third condition (Condition3) for your search.
- 6 From the Select View list, select an appropriate view.

Note: The view determines how users are presented when a user search is completed. The General view shows general information about the user

(for example, his or her title, department, and name). The Administrative view shows the user's administrative capabilities (for example, his or her password retry count and access class). The Messaging view shows the user's mailbox capabilities (for example, mailbox class or the Target Number for a paging device).

- 7 Click Search Now.

Result: The Users window appears, showing the results of the user search.

See also

- [“Specifying search criteria” on page 71.](#)
- [“Restricting a user search” on page 75.](#)
- [“Modifying and reusing your latest user search” on page 77.](#)

Restricting a user search

Introduction

Your first search might be too general to be of use. To reduce the number of matches found in a search, reduce the scope of your search.

Example

There are 30 users named Smith in your system. The Smith you need to find is a manager.

To find the manager named Smith, search for Last Name is Smith AND Title is manager.

Before you begin

You must have already specified at least one set of search conditions and run one search. If you have not, see [“Specifying search criteria,” on page 71](#).

Getting there CallPilot System > User Administration > Users

To restrict a user search

- 1 Click All conditions. This means that only users who meet all the conditions set in your search will be included in the search results.
- 2 From the Search Criteria list in the Condition2 row, select the additional criteria with which you want to search.
- 3 From the Operator list in the Condition2 row, select an appropriate operator.
- 4 In the Value list in the Condition2 row, type an appropriate value.
- 5 If desired, fill in the Search Criteria, Operator, and Value to add third condition (Condition3) for your search.
- 6 From the Select View list, select an appropriate view.

Note: The view determines how users are presented when a user search is completed. The General view shows general information about the user (for example, his or her title, department, and name). The Administrative

view shows the user's administrative capabilities (for example, his or her password retry count and access class). The Messaging view shows the user's mailbox capabilities (for example, mailbox class or the Target Number for a paging device).

- 7 Click Search Now.

Result: The Users window appears, showing the results of the user search.

See also

- [“Specifying search criteria” on page 71.](#)
- [“Broadening a user search” on page 73.](#)

Modifying and reusing your latest user search

Introduction

If you want to modify the search (for example, widen or narrow the scope), you can retrieve your most recent search criteria settings using the Open Search menu command.

Before you begin

You must have already specified at least one set of search conditions and run one search. If you have not, see [“Specifying search criteria,” on page 71](#).

Getting there CallPilot System > User Administration > Users

To retrieve your latest user search

- 1 On the File menu, click Open Search.
Result: The Search Users dialog box appears with the same conditions you set the last time you used it.
- 2 Change the search settings as desired.
- 3 Click Search Now.

See also

- [“Saving a user search” on page 78](#).
- [“Running a saved user search” on page 79](#).
- [“Deleting a saved user search” on page 80](#).

Saving a user search

Introduction

If you search for a specific group of users regularly, you can save the search criteria for this search. When you save a user search, you bypass resetting all the search criteria and settings each time you want to perform this search. The saved search is added to the Saved User Searches window.

Getting there CallPilot System > User Administration > Users

To save a user search

- 1 After you have performed the search you want to save, select File > Save Search.

Result: The Save Query dialog box appears.

- 2 In the Enter Query Name box, type a name for the search.
- 3 Click OK.

Note: If you save a user search while the Saved User Searches window is open, refresh this screen to see your newly saved search added to the list.

See also

- [“Modifying and reusing your latest user search” on page 77.](#)
- [“Running a saved user search” on page 79.](#)
- [“Deleting a saved user search” on page 80.](#)

Running a saved user search

Introduction

When you run a saved user search, you bypass the process of resetting the search criteria and settings each time you perform a particular search.

Tip

If the saved search you want to run is not listed in the Saved User Searches window, try clicking Refresh. This updates your display to show any recently saved searches.

Getting there CallPilot System > User Administration > Saved User Searches

To run a saved user search

Double-click the name of the saved search you want to run.

Result: The Users window appears, displaying the results of your search.

See also

- [“Saving a user search” on page 78.](#)
- [“Deleting a saved user search” on page 80.](#)

Deleting a saved user search

Introduction

If the criteria specified in the saved search becomes obsolete, you can remove the search from the system.

Getting there CallPilot System > User Administration > Saved User Searches

To delete a saved user search

- 1 Click the saved search you want to delete.
- 2 On the File menu, click Delete.
Result: A confirmation dialog box appears, asking you to confirm the deletion.
- 3 Click Yes.
Result: The Saved User Searches dialog box reappears with the updated list of user searches.

Section C: Managing user mailboxes

In this section

<u>Changing a user's personal information</u>	<u>82</u>
<u>Adding/changing/canceling an administrator's access capability</u>	<u>83</u>
<u>Temporarily preventing administrators from accessing the desktop</u>	<u>85</u>
<u>Restoring a user's administrative desktop access</u>	<u>87</u>
<u>Resetting a user's administrative password</u>	<u>89</u>
<u>Changing a user's mailbox properties</u>	<u>90</u>
<u>Deleting a user from the system</u>	<u>91</u>
<u>Printing user account details</u>	<u>92</u>

Changing a user's personal information

Introduction

If a user changes his or her name or position within your company, you can change some or all of his or her personal user information.

Use the General Information tab to change a user's first name, last name, initials, title, and department. You can also modify any comments you have recorded about the user.

Before you begin

Run a search to locate the record for the user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To change a user's personal information

- 1 Click the user whose information you want to change.
- 2 On the File menu, click Properties.
Result: The user's property sheet appears.
- 3 Click the General tab if it is not already selected.
- 4 Type new entries into any box whose value you need to change for this user. From this tab you can change
 - First Name
 - Initials
 - Last Name
 - Comments
 - Title
 - Department
- 5 Click Save.

Adding/changing/canceling an administrator's access capability

Introduction

If a user who is also an administrator changes his or her position within your company, you can modify his or her access class. You can also grant or cancel administrative access for an existing user through this procedure.

Example

One of your managers changed departments and is no longer responsible for managing users in the system. Instead, he or she is responsible for system maintenance. To ensure that the manager has access to the necessary maintenance-related programs, you must assign him or her to an access class that gives access to the appropriate functions.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To give administrative capability to a user

- 1 Click the user to whom you want to give administrative capability.
- 2 On the File menu, click Properties.
Result: The user's property sheet appears.
- 3 On the left side of the sheet, click the check box beside Admin Capability in the file tree.
- 4 Click the Admin tab.
- 5 From the Access Class list, select the user's administrative access class.
- 6 Click Save.

Result: The Users window reappears with the updated user list.

To change a user's administrative access class

- 1 Click the user whose access class you want to change.
- 2 On the File menu, click Properties.
Result: The user's property sheet appears.
- 3 Click the Admin tab.
- 4 From the Access Class list, select the new access class.
- 5 Click Save.

Result: The Users window reappears with the updated user list.

To cancel administrative capability for a user

- 1 Click the user whose administrative capability you want to cancel.
- 2 On the File menu, click Properties.
Result: The user's property sheet appears.
- 3 On the left side of the sheet, clear the check box beside Admin Capability in the file tree.
- 4 Click Save.

Result: The Users window reappears with the updated user list.

See also

- [“Temporarily preventing administrators from accessing the desktop” on page 85.](#)
- [“Restoring a user's administrative desktop access” on page 87.](#)
- [“Resetting a user's administrative password” on page 89.](#)

Temporarily preventing administrators from accessing the desktop

Introduction

If you require sole access to the system or to parts of the system, you can temporarily prevent other administrative users from accessing the CallPilot Administration Client window.

Example

You need to run diagnostics on maintenance-related objects within the system. To prevent users from accessing these objects while they are in use, you can temporarily lock out any users who have access to the CallPilot Administration Client window.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To prevent a user from accessing the desktop

1 Click the user you want to prevent from accessing the desktop.

2 On the File menu, click Properties.

Result: The selected user's property sheet appears.

3 Click the Admin tab.

4 Click Lock Out.

Result: The Lock Out label changes to Restore.

5 Click Save.

Result: The Users window reappears with the updated user list.

See also

- [“Adding/changing/canceling an administrator’s access capability” on page 83.](#)
- [“Restoring a user’s administrative desktop access” on page 87.](#)
- [“Resetting a user’s administrative password” on page 89.](#)

Restoring a user's administrative desktop access

Introduction

If a user who is an administrator fails three times to enter the correct user ID and password, he or she is locked out of the CallPilot Administration Client window. Only a user with the correct administrative permissions can restore access to a user who has been locked out.

Also, if a user has been locked out by an administrator, you might need to restore his or her access to the CallPilot Administration Client window.

Note: This procedure deals with users whose administrative access has been locked out temporarily. For information on granting administrative access to a user who did not have it before, see [“Adding/changing/canceling an administrator's access capability” on page 83](#).

Before you begin

You must run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To restore a user's desktop access

- 1 Click the user for whom you want to restore desktop access.
 - 2 On the File menu, click Properties.
- Result:** The selected user's property sheet appears.
- 3 Click the Admin tab.
 - 4 Click Restore.

Result: The Restore label changes to Lock Out.

- 5 Click Save.

Result: The Users window reappears with the updated user list.

See also

- [“Adding/changing/canceling an administrator’s access capability” on page 83.](#)
- [“Temporarily preventing administrators from accessing the desktop” on page 85.](#)
- [“Resetting a user’s administrative password” on page 89.](#)

Resetting a user's administrative password

Introduction

If a user forgets his or her system password, you can reset it to the default password.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To reset a user's password

1 Click the user whose password you want to reset.

2 On the File menu, click Properties.

Result: The selected user's property sheet appears.

3 Click the Admin tab.

4 Click Reset Password.

Result: A confirmation dialog box appears, displaying the new password and asking you to confirm the reset.

5 Click Yes.

6 Click Save.

Result: The Users window reappears with the updated user list.

See also

- [“Adding/changing/canceling an administrator's access capability” on page 83](#).
- [“Temporarily preventing administrators from accessing the desktop” on page 85](#).
- [“Restoring a user's administrative desktop access” on page 87](#).

Changing a user's mailbox properties

Introduction

You can change any existing user mailbox properties, with the exception of required fields and the Volume ID.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To change a local user's mailbox properties

- 1 Select the user whose mailbox properties you want to change.
- 2 On the File menu, click Properties.
Result: The selected user's property sheet appears.
- 3 Click the Mailbox tab.
- 4 Change the mailbox settings as required.
- 5 When you have finished modifying the desired settings, click Save.

See also

See “Setting up user templates” in the *Administrator's Guide* for more information on user mailbox settings.

Deleting a user from the system

Introduction

If a user has left your company, remove the user from your system for security reasons. If you do not delete these users, your system is vulnerable to hacking.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To delete a user

- 1 Click the user you want to delete.
- 2 On the File menu, click Delete.

Result: A dialog box appears, asking you to confirm the deletion.

- 3 Click Yes.

Result: The Users window reappears with the updated user list.

See also

- [“Printing user account details” on page 92](#).
- [“Checking when a user last used a mailbox” on page 101](#).

Printing user account details

Introduction

If you require a printed copy for your records, you can print a report listing user account details for one user or a group of users.

Before you begin

Run a search to locate the selected user or users. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To print a list of all users listed in the Users window

- 1 On the File menu, click Print.

Result: The Print dialog box appears.

- 2 Click All for the print range.

- 3 Click OK.

Result: The list prints on your default printer.

To print detailed information about selected users

- 1 Select the user(s) for whom you want to print information.

- 2 On the File menu, select Print.

Result: The Print dialog box appears.

- 3 Click Selection for the print range.

- 4 Click OK.

Result: The list prints on your default printer.

Section D: Frequently performed tasks

In this section

<u>Reenabling a disabled mailbox</u>	<u>94</u>
<u>Resetting a user's mailbox password</u>	<u>95</u>
<u>Increasing a user's mailbox storage space</u>	<u>96</u>
<u>Enabling or disabling Autologon</u>	<u>97</u>
<u>Checking how much storage space a user has left</u>	<u>98</u>
<u>Checking if a user has recorded greetings</u>	<u>99</u>
<u>Checking when a user last used a mailbox</u>	<u>101</u>
<u>Checking invalid logon attempts to a mailbox</u>	<u>102</u>

Reenabling a disabled mailbox

Introduction

Reenable a disabled mailbox that might have been temporarily unused or was disabled after too many invalid logon attempts.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To reen able a user mailbox

- 1 Select the user whose mailbox you want to reen able.
- 2 On the File menu, click Properties.
Result: The selected user’s property sheet appears.
- 3 Click the Security tab.
- 4 To reen able a user mailbox, select Enabled from the Logon status box.
- 5 Click Save.

Resetting a user's mailbox password

Introduction

Reset a user's mailbox password if the user has forgotten the password.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To reset the password for a user mailbox

- 1 Select the user whose password you want to reset.
- 2 On the File menu, click Properties.
Result: The selected user's property sheet appears.
- 3 Click the Security tab.
- 4 Click Set password.
- 5 In the Set password box, type the password for the user's mailbox.
Note: Remember that a mailbox password is expressed as a number. The user can remember it in alphabetic terms, but you must enter it here as a number. For example, “PASSWORD” = 72779673.
- 6 In the Confirm password box, type the password again.
- 7 Click OK.
- 8 Click Save on the User Properties property sheet and return to the Users list.

Increasing a user's mailbox storage space

Introduction

Increase the amount of storage space for a user's mailbox if the user needs to retain a greater volume of messages. To do this, reassign the user to a mailbox class that allocates more message storage space.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To reassign a user's mailbox class to one that provides more mailbox storage

- 1 Select the user whose mailbox class you want to change.
- 2 On the File menu, click Properties.
Result: The selected user's property sheet appears.
- 3 Click the Mailbox tab.
- 4 In the Mailbox class list, select another mailbox class that provides the desired amount of storage space.
- 5 To confirm that the new mailbox class provides more mailbox storage, click Details to view the settings for the mailbox class you chose.
- 6 Click Save in the User Properties property sheet.

See also

For more detailed information about mailbox classes, see “Configuring mailbox capabilities for a user group” in the *Administrator's Guide*.

Enabling or disabling Autologon

Introduction

Enable or disable a user's ability to access their mailbox without having to log on or enter a password.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To enable or disable Autologon for a user mailbox

- 1 Select the user for whom you want to enable or disable Autologon.
- 2 On the File menu, click Properties.
Result: The selected user's property sheet appears.
- 3 Click the DN's tab.
- 4 To enable Autologon for an Extension DN, check the Autologon allowed check box beside that DN.
- 5 To disable Autologon for an Extension DN, clear the Autologon allowed check box beside that DN.
- 6 Click Save.

Note: To use the Autologon feature, users must be logged on to their mailbox and press 80 for mailbox options, and then 4 for Autologon. Users can then toggle Autologon on (press 1) or off (press 2).

Checking how much storage space a user has left

Introduction

Check the amount of remaining storage space a user has to determine if he or she needs more total storage. You might need to reassign the user to another mailbox class that provides greater storage space.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To view the status of a user mailbox

- 1 Select the user whose mailbox status you want to check.
- 2 In the File menu, click Properties.
Result: The selected user's property sheet appears.
- 3 Click the Status tab.
- 4 In the Storage used box, confirm the storage space used in the user mailbox.
- 5 In the Total available box, confirm the message storage space that remains in the user mailbox.
- 6 In the Total system resources box, confirm the storage space that is available to the user mailbox, which includes messages and all other individual greetings and personal distribution lists.

See also

For more information about changing a mailbox class to increase storage space, see “Configuring mailbox capabilities for a user group” in the *Administrator's Guide*.

Checking if a user has recorded greetings

Introduction

Check if the user has recorded personal greetings. If not, you can record one on behalf of the user.

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

Getting there CallPilot System > User Administration > Users

To view a user's greeting status

- 1 Select the user whose greeting status you want to check.
- 2 In the File menu, click Properties.
Result: The selected user's property sheet appears.
- 3 Click the Status tab.
- 4 In the Personal verification box, check if a spoken name is associated with the user mailbox.
- 5 In the Internal personal greeting box, check if there is a mailbox greeting that other local users hear.
- 6 In the External personal greeting box, check if there is a mailbox greeting that external callers hear.
- 7 In the Temporary absence greeting box, check if there is a temporary greeting for the user mailbox while the user is away from work. Most mailboxes only occasionally require Temporary absence greetings.
- 8 In the Temporary absence greeting expiry box, confirm when the temporary mailbox greeting, if there is one, will stop playing to callers and revert to the regular mailbox greeting.

See also

For more information about recording a greeting on the user's behalf, see "Adding and deleting users and directory entries" in the *Administrator's Guide*.

Checking when a user last used a mailbox

Introduction

Check when a mailbox was last used to determine if it has been inactive long enough to warrant being deleted. Unused mailboxes are a security risk because hackers can use them without being noticed for a long time.

Note: CallPilot does not update the last logon time of a mailbox when a user logs on from a desktop client. This can cause an Administrator to delete a mailbox that looks inactive but is actually being used from a desktop client. Check to see if the mailbox is being used from a desktop client before deleting it.

Getting there CallPilot System > User Administration > Users

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

To check the last mailbox access

- 1 Select the user whose most recent mailbox access you want to check.
- 2 In the File menu, click Properties.
Result: The selected user's property sheet appears.
- 3 Click the Security tab.
- 4 Check the Time of last login box.

See also

For more information on deleting a user mailbox, see [“Deleting a user from the system” on page 91](#).

Checking invalid logon attempts to a mailbox

Introduction

Check how many failed logon attempts have been made on a mailbox to determine whether to monitor the mailbox for suspicious activity. You might also want to take further security measures to protect the system. Frequent invalid logon attempts often indicate that a hacker is trying to get into the mailbox by testing passwords.

Getting there CallPilot System > User Administration > Users

Before you begin

Run a search to locate the selected user. See [“Overview” on page 66](#).

To check the number of invalid logon attempts

- 1 Select the user whose mailbox logon attempts you want to check.
- 2 In the File menu, click Properties.
Result: The selected user's property sheet appears.
- 3 Click the Security tab.
- 4 Check the Invalid logon attempts box. You can disable the mailbox, or you can monitor it using Hacker Monitoring.

Chapter 5

Creating and maintaining shared distribution lists

In this chapter

Overview	105
Section A: About distribution lists	107
What is a distribution list?	108
Shared distribution lists versus personal distribution lists	110
What kinds of users can be included in shared distribution lists?	111
Guidelines for creating shared distribution lists	112
Section B: Setting up shared distribution lists	115
Opening Shared Distribution Lists	116
Setting up a shared distribution list	117
Creating and labeling the shared distribution list	119
Recording a name for the shared distribution list	120
Choosing the type of user to add to the shared distribution list	121
Using the Search Users tool to collect users for an SDL	122
Adding a single user to the shared distribution list	123
Adding all users to the shared distribution list	124
Adding a user with a known Callback DN or mailbox number	125
Creating a remote user for the shared distribution list	126
Defining the mailbox settings for a remote user	127
Recording a spoken name for a remote user	129
Importing a WAV file for the remote user's name	130
Creating a directory entry for the shared distribution list	131

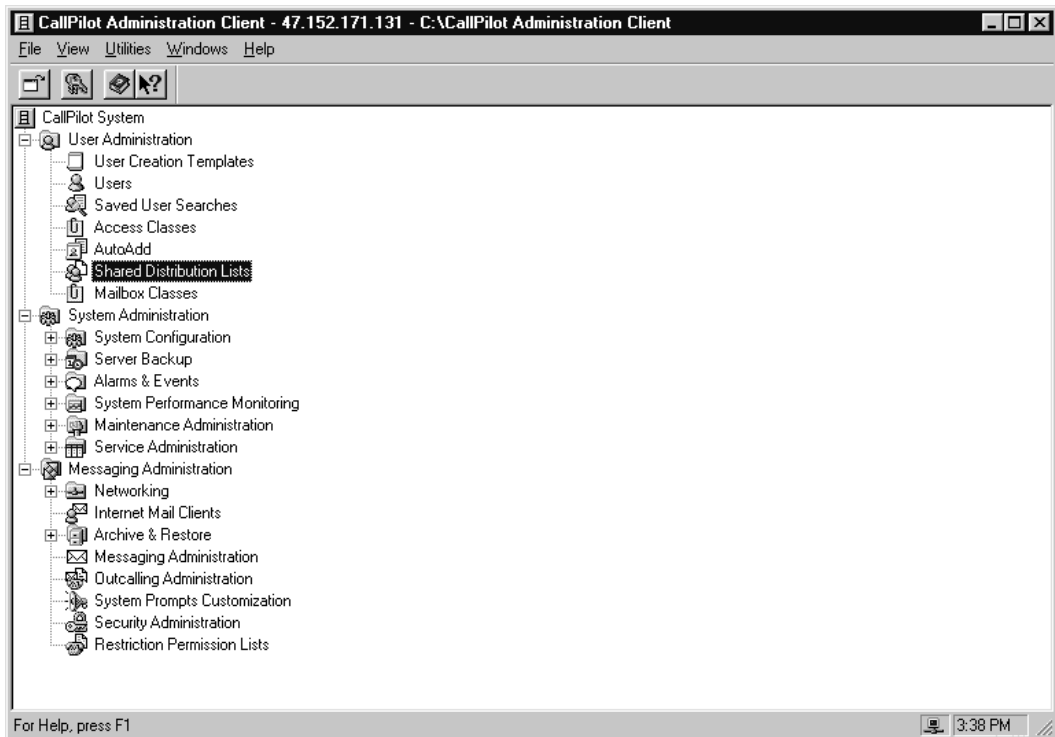
<u>Defining the settings for a directory entry</u>	<u>132</u>
<u>Recording a spoken name for a directory entry</u>	<u>133</u>
<u>Importing a WAV file for a directory entry</u>	<u>134</u>
<u>Viewing a shared distribution list</u>	<u>135</u>
<u>Viewing or changing a shared distribution list</u>	<u>136</u>
<u>Deleting a user from a shared distribution list</u>	<u>137</u>
<u>Deleting a shared distribution list</u>	<u>138</u>
<u>Printing shared distribution lists</u>	<u>139</u>

Overview

Introduction

This chapter explains shared distribution lists (SDLs), how to set them up, and the ways in which users can use them. In addition, this chapter suggests how to make SDLs available to other administrators or users.

You access your shared distribution lists tools from the CallPilot Administration Client as shown below.



Section A: About distribution lists

In this section

What is a distribution list?	108
Shared distribution lists versus personal distribution lists	110
What kinds of users can be included in shared distribution lists?	111
Guidelines for creating shared distribution lists	112

What is a distribution list?

Definition

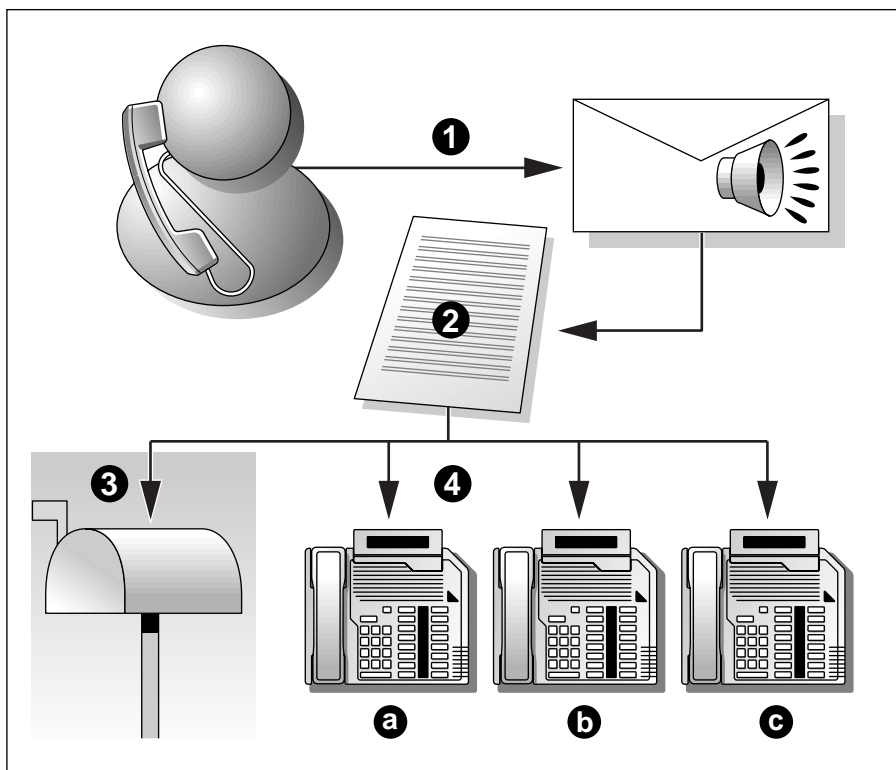
A distribution list is a mailing list that allows you to send the same message to a group of people. After you create and save a distribution list, you can reuse it whenever you need to send messages to the same group of people.

Creation of a distribution list involves assigning a unique number and title to the list and specifying the mailbox numbers you want to include in the list.

How messages are sent to a distribution list

When you compose a message, you specify the distribution list number as you would any mailbox number. Then, when you send your message, it is deposited in every mailbox or sent to every phone number in the list.

The following diagram shows how messages are sent to a distribution list.



G100904

1. A user composes a message.
2. The user selects an SDL.
3. The SDL sends the voice message to one or more mailboxes.
4. The SDL also sends voice messages to various external phone numbers.

Shared distribution lists versus personal distribution lists

Two types of lists

There are two types of distribution lists: shared distribution lists (SDLs) and personal distribution lists (PDLs). This chapter deals with SDLs.

Shared distribution list

As an administrator, you add an SDL through the Shared Distribution Lists program. Create an SDL so that users can send messages to all of the addresses in the SDL. A user must belong to a mailbox class that provides permission to use SDLs.

You can add up to 150 SDLs, each containing up to 999 mailboxes.

Personal distribution list

CallPilot users create PDLs from their phonesets. A PDL is available only to the user who created it. The PDL allows the user to send a recorded message to all the mailboxes contained in the list.

A user can create up to 99 personal distribution lists, each containing up to 200 mailboxes.

Restrictions on personal distribution lists

Each SDL is one address, regardless of the number of entries on the list. However, each entry on a PDL is one address. Therefore, an SDL with ten entries is one address, while a PDL with ten entries is ten addresses.

There are some limitations on the total number of addresses to which an outgoing message can be sent using PDLs. If a user tries to send a message to a number of distribution lists, he or she may get the following message if the maximum address size of the message is exceeded: “Your command cannot be completed at this time. Please try again, or contact your administrator.” The message is deleted, and the user is positioned at the next message in the mailbox (or at the end of the mailbox) and can use other commands normally.

What kinds of users can be included in shared distribution lists?

Kinds of users

You can include the following kinds of users in an SDL because each one has a recognizable and unique name and mailbox on the system:

- local users
- directory entries on the local site
- remote users

Impact of Networking on SDLs

To include a remote user site in an SDL, you must define the site and location in your messaging network and have Networking installed.

To include users at remote sites in a CallPilot network, you must define them as remote voice users in the local database. The following types of numbers do not have mailboxes associated with them, so they cannot be included in an SDL:

- remote notification (RN) targets
- nonusers who require Delivery to Telephone (DTT)

Guidelines for creating shared distribution lists

Introduction

SDLs allow users to send messages to a group of numbers. There are some storage capacity restrictions based on the number of members on the list and the size of the distributed message.

Restrictions on distribution lists

The following restrictions are placed on distribution list numbers:

- An SDL cannot be assigned a number between 1 and 99. These numbers are reserved for PDLs.
- Each SDL must have a unique distribution list number.
- An SDL number must not conflict with any dialing plan prefixes or codes.
- An SDL number cannot be the same as any mailbox number, including the broadcast mailbox number. The default broadcast mailbox number is 5555.
- An SDL number cannot be the same as a directory entry user's DN. If an SDL number and a directory entry user number are the same, the SDL number takes priority when a list is created.
- An SDL cannot be nested inside another SDL.

Message number and size

The number of addresses to which a user can successfully send a message simultaneously depends on the size of the message, as shown in the following table.

Note: Each SDL is one address, regardless of the number of entries on the list. Each entry on a PDL is one address. Therefore, an SDL with ten entries is one address, while a PDL with ten entries is ten addresses.

Length of message and number of addresses

A message and its address list have limited storage space. Therefore, the longer the message is, the fewer addresses can be contained in the SDL.

Length of message	Number of addresses
90 minutes	290
60 minutes	350
10 minutes	425
1 minute	440

Dealing with multimedia messages

Users can send multimedia messages with an SDL. Users can assume that internal numbers all have voice and fax-receiving capabilities.

However, you cannot assume that external numbers can receive multimedia messages. Create an SDL of external phone numbers for voice messages and a second SDL of external fax numbers.

Section B: Setting up shared distribution lists

In this section

Opening Shared Distribution Lists	116
Setting up a shared distribution list	117
Creating and labeling the shared distribution list	119
Recording a name for the shared distribution list	120
Choosing the type of user to add to the shared distribution list	121
Using the Search Users tool to collect users for an SDL	122
Adding a single user to the shared distribution list	123
Adding all users to the shared distribution list	124
Adding a user with a known Callback DN or mailbox number	125
Creating a remote user for the shared distribution list	126
Defining the mailbox settings for a remote user	127
Recording a spoken name for a remote user	129
Importing a WAV file for the remote user's name	130
Creating a directory entry for the shared distribution list	131
Defining the settings for a directory entry	132
Recording a spoken name for a directory entry	133
Importing a WAV file for a directory entry	134
Viewing a shared distribution list	135
Viewing or changing a shared distribution list	136
Deleting a user from a shared distribution list	137
Deleting a shared distribution list	138
Printing shared distribution lists	139

Opening Shared Distribution Lists

Introduction

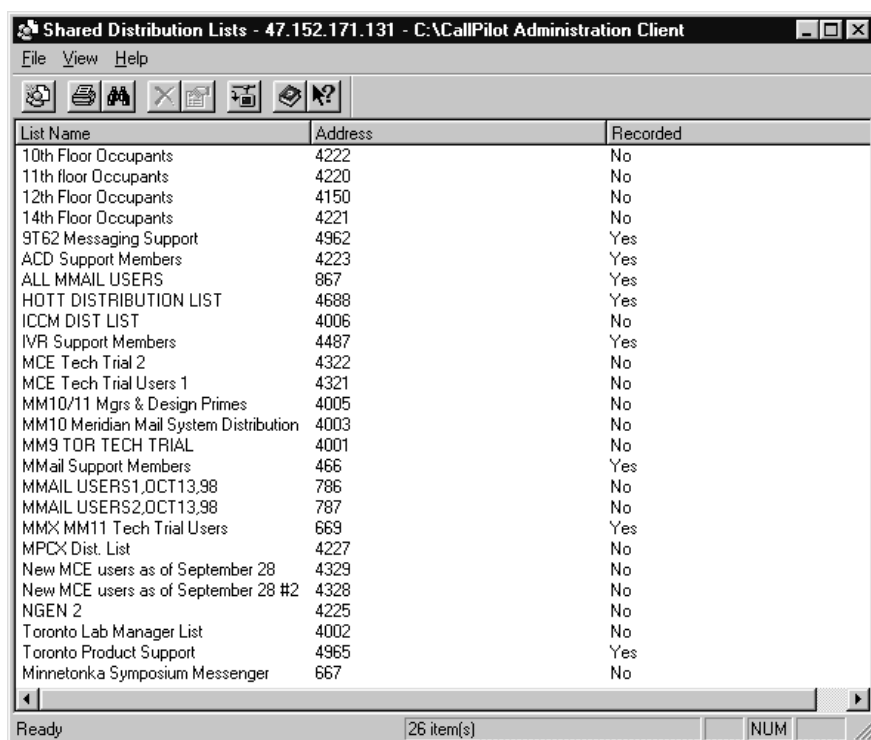
Open Shared Distribution Lists to create a new SDL or maintain an existing one.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To open Shared Distribution Lists

Double-click Shared Distribution Lists.

Result: The Shared Distribution Lists window appears.



Setting up a shared distribution list

Introduction

Create an SDL so that users can send a common message to a group of CallPilot users.

The following procedure is a compilation of all of the smaller procedures involved in creating an SDL.

To set up an SDL

- 1 To create and label the new SDL, follow these procedures.
 - a. [“Creating and labeling the shared distribution list” on page 119.](#)
 - b. [“Recording a name for the shared distribution list” on page 120.](#)
- 2 Some SDLs contain users who have a particular user mailbox field entry in common (for example, an SDL for all users whose Department is Sales). To generate a list of users based on a search for user field entries, follow this procedure.
 - [“Using the Search Users tool to collect users for an SDL” on page 122.](#)
- 3 To add local users to the SDL, choose from one of the following methods:
 - [“Adding a single user to the shared distribution list” on page 123.](#)
 - [“Adding all users to the shared distribution list” on page 124.](#)
 - [“Adding a user with a known Callback DN or mailbox number” on page 125.](#)
- 4 To add a remote user to the SDL, follow these procedures:
 - a. [“Creating a remote user for the shared distribution list” on page 126.](#)
 - b. [“Defining the mailbox settings for a remote user” on page 127.](#)
 - c. [“Recording a spoken name for a remote user” on page 129](#) or [“Importing a WAV file for the remote user’s name” on page 130.](#)
- 5 To add a directory entry user to the distribution list, follow these procedures:
 - a. [“Creating a directory entry for the shared distribution list” on page 131.](#)
 - b. [“Defining the settings for a directory entry” on page 132.](#)

- c. [“Recording a spoken name for a directory entry” on page 133](#) or [“Importing a WAV file for a directory entry” on page 134](#).

Creating and labeling the shared distribution list

Introduction

Define the name, number, and comments to identify a distribution list.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To create and label the SDL

- 1 From the File menu, select New.
Result: The New SDL Properties property sheet appears.
- 2 In the List Name box, type a unique name for the SDL.
- 3 In the Address box, type the unique access number users dial to send messages to members of the SDL.
- 4 In the Comments box, type an optional description of the SDL.
- 5 Click Save.

See also

For more detailed information on SDLs, see [“Guidelines for creating shared distribution lists” on page 112](#).

Recording a name for the shared distribution list

Introduction

Record a name that identifies the list when its number is entered during message composition.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To record a name for the SDL

- 1 Select the SDL for which you want to record a name.
- 2 In the File menu, click Properties.
Result: The SDL Properties property sheet appears.
- 3 Click Record.
Result: The Specify Phoneset dialog box appears.
- 4 In the Enter a phone number box, type the phone number of the telephone you want to use for recording.
- 5 Answer the telephone when it rings.
Result: The Voice Recorder dialog box appears.
- 6 Click Record.
- 7 Speak an appropriate name for the distribution list into the phoneset.
- 8 Click Stop to stop the recording.
- 9 To review the recorded title, click Play.
- 10 Click Done to save the recording and return to the SDL Properties property sheet.

Choosing the type of user to add to the shared distribution list

Introduction

Select both a type of user to add and a way to add the user to your SDL by referring to the appropriate procedure in this section.

To choose the type of user to add to the SDL

To	See
add a single local user to the list	“Adding a single user to the shared distribution list” on page 123.
add all the users from the Users list	“Adding all users to the shared distribution list” on page 124.
add a local user with a known Callback DN or mailbox number	“Adding a user with a known Callback DN or mailbox number” on page 125.
search for user on the system based on criteria you define	“Using the Search Users tool to collect users for an SDL” on page 122.
create a remote user if your system is networked	“Creating a remote user for the shared distribution list” on page 126.
create a directory entry user	“Creating a directory entry for the shared distribution list” on page 131.

Using the Search Users tool to collect users for an SDL

Introduction

Use Search Users to find and collect users based on specific criteria. Then select users from the search to include in an SDL.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To generate a list of users for the SDL

- 1 Select the SDL for which you want to generate a list of users.
- 2 In the File menu, click Properties.
Result: The SDL Properties property sheet appears.
- 3 Click Search Users. The Search Users dialog box appears.

Note: For detailed information on how to use the Search Users dialog box to isolate particular users or groups of users, see [“What is a user search?” on page 67](#).

Adding a single user to the shared distribution list

Introduction

Select a user from the list of available users, and add him or her to the SDL.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To add a local user mailbox to the SDL

- 1 Select the SDL to which you want to add a local user.
- 2 In the File menu, click Properties.

Result: The SDL Properties property sheet appears.

Note: In the SDL Properties property sheet, if you select a user mailbox, it appears in list on the right side. It no longer appears in the list of available user mailboxes on the left side.

- 3 Use the Search Users feature to isolate one user or a group of users. For more information, see [“Using the Search Users tool to collect users for an SDL” on page 122](#).

Note: You do not need to isolate only the user(s) that you intend to add to the SDL. The purpose of the user search is to narrow the list so that you can easily find the user(s) you want.

- 4 Select the desired user in the Users box.
- 5 Click Add to include the user in the SDL.
- 6 Repeat steps [4](#) and [5](#) until you have added all the users you want to add.
- 7 Click Save to save your SDL.

Adding all users to the shared distribution list

Introduction

You can add all or most of the users found in the user search to the distribution list in one step. The list can contain local users, remote users, and directory entry users.

Tip: If you want to add most but not all users in the Users list, add all of them and then remove the selected few you do not want to include in the SDL. For instructions on removing users from the SDL, see [“Deleting a user from a shared distribution list” on page 137](#).

Before you begin

Select the SDL to which you want to add users, open its SDL Properties property sheet, and run a User Search to isolate the desired users on the screen.

For more information, see [“Using the Search Users tool to collect users for an SDL” on page 122](#).

Getting there CallPilot System > User Administration > Shared Distribution Lists

To add all the users from the generated list to the SDL

- 1 Click Add all >> to include all the users in the User to add box in the SDL.
- 2 Click Save to save the SDL and return to the main window.

Adding a user with a known Callback DN or mailbox number

Introduction

You can add a user who is not in the list of users to the SDL if you know that user's mailbox number or callback DN. This option is useful if you generate a list of users with the search mechanism, and you then wish to include a few more users who were not included in the generated list but who should be in the SDL.

Before you begin

Select the SDL to which you want to add users and open its SDL Properties property sheet.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To add a local user to the SDL whose Callback DN or mailbox number is already known

- 1 Click Add user.
Result: The Add a user to distribution list dialog box appears.
- 2 If you know the user's mailbox number, click the Mailbox number button, and type the number into the box beside it.
- 3 If you know the user's Callback DN, click the Callback DN button, and type the DN into the box beside it.
- 4 Click Save to add the user, and return to the Properties tab.

Creating a remote user for the shared distribution list

Introduction

If you want to add a user at another networking location to the SDL, but that user has not yet been added to the database as a remote user, you can do both at the same time.

Before you begin

Select the SDL to which you want to add users and open its SDL Properties property sheet.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To create a remote user for the SDL

- 1 Click the New remote user button for the selected user to appear in the Distribution list contents box.
- 2 In the First name box, type a first name for the user.
- 3 In the Initial(s) box, type a middle initial for the user.
- 4 In the Last name box, type a last name for the user.
- 5 To include extra information to identify the remote user more easily when administering the system, in the Comments box, type the information.
- 6 In the Title box, type the user's business title.
- 7 In the Department box, type the name of the user's department.
- 8 To configure the mailbox settings for this remote user, follow the procedure in ["Defining the mailbox settings for a remote user" on page 127](#).

Defining the mailbox settings for a remote user

Introduction

Set up the remote user's mailbox number and its associated settings.

Before you begin

Select the SDL to which you want to add users and open its SDL Properties property sheet. You must also follow the procedure in [“Creating a remote user for the shared distribution list” on page 126](#).

Getting there CallPilot System > User Administration > Shared Distribution Lists > File > Properties (New remote user button) > Add Remote User > Settings tab

To define the settings for a remote user

- 1 In the Mailbox number box, type the directory number local users require to dial the remote user.
- 2 In the first Extension DN box, type the primary telephone number of the user's mailbox.
Note: If the mailbox has no more extension numbers associated with it, go to step [4](#).
- 3 To specify other extension numbers that the user has, in the other Extension DN boxes, type the extension numbers.
- 4 To define the number Call Sender uses to call back this user, in the Callback DN box, type a DN
Note: The default is the primary extension DN.
- 5 To let external callers call the remote user by spelling his or her name, make sure the Name dialable by external callers check box is checked.

- 6 To have the system delete the remote user if he or she is no longer frequently accessed or sent messages, make sure the Temporary user check box is checked.
- 7 To record a personal verification for this remote user, follow the procedure in [“Recording a spoken name for a remote user” on page 129](#).

Recording a spoken name for a remote user

Introduction

Record a personal verification for the remote user that identifies the user when someone is sending a message or composing a distribution list.

Before you begin

Select the SDL to which you want to add users and open its SDL Properties property sheet. You must also follow the procedures in [“Creating a remote user for the shared distribution list” on page 126](#) and [“Defining the mailbox settings for a remote user” on page 127](#).

Getting there CallPilot System > User Administration > Shared Distribution Lists > File > Properties (New remote user button) > Add Remote Users > Settings tab

To record a name

- 1 Click Record.
Result: The Specify Phoneset dialog box appears.
- 2 In the Enter a phone number box, type the phone number of the phoneset you want to use for recording.
- 3 Answer the phoneset when it rings.
Result: The Voice Recorder dialog box appears.
- 4 Click Record.
- 5 Speak the name for the remote user into the phoneset.
- 6 Click Stop.
- 7 To review the recorded name, click Play.
- 8 If you are happy with the recording, click Done to return to the Settings tab.
- 9 If you are unhappy with the recording, repeat steps [4](#) through [6](#).

Importing a WAV file for the remote user's name

Introduction

Import a WAV file for the Personal Verification that identifies a remote user. Callers and message senders hear this personal verification during call answering and various messaging sessions.

Before you begin

Select the SDL to which you want to add users and open its SDL Properties property sheet. You must also follow the procedures in [“Creating a remote user for the shared distribution list” on page 126](#) and [“Defining the mailbox settings for a remote user” on page 127](#).

Getting there CallPilot System > User Administration > Shared Distribution Lists > File > Properties (New remote user button) > Add Remote User > Settings tab

To import a WAV file for the remote user's spoken name

- 1 To import a WAV file, click Import.
- 2 Select the file that contains a recording of the user's spoken name.
- 3 Click Open.

Creating a directory entry for the shared distribution list

Introduction

If you want to add a directory entry user to the SDL, but that user has not yet been added to the database, you can do both at the same time.

Note: Although a directory entry has no mailbox, it receives a message from the shared distribution list in the same way as the Delivery to Telephone message is received by phone numbers that are not on the system.

Before you begin

Select the SDL to which you want to add users and open its SDL Properties property sheet.

Getting there CallPilot System > User Administration > Shared Distribution Lists > File > Properties

To create a new directory entry user and add it to the SDL

- 1 Click New directory entry user.
- 2 In the First name box, type a first name for the user.
- 3 In the Initial(s) box, type a middle initial for the user.
- 4 In the Last name box, type a last name for the phoneset that easily identifies its users or its location.
- 5 To include any extra information to identify the directory entry more easily when administering the system, in the Comments box, type the information.
- 6 In the Title box, type the user's business title.
- 7 In the Department box, type the name of the user's department.
- 8 To configure the settings for the new directory entry user, follow the procedure in ["Defining the settings for a directory entry" on page 132](#).

Defining the settings for a directory entry

Introduction

Set up the directory entry's extension DNs and its associated settings.

Before you begin

Select the SDL to which you want to add users and open its SDL Properties property sheet. You must also follow the procedure in [“Creating a directory entry for the shared distribution list” on page 131](#).

Getting there CallPilot System > User Administration > Shared Distribution Lists > File > Properties (New directory entry user button) > Add Directory Entry User > Settings tab

To define the settings for a directory entry

- 1 In the first Extension DN box, type the primary number associated with the user.
Note: If the user has no more extension numbers, go to step 3.
- 2 To specify other extension numbers that the user also has, in the following Extension DN boxes, type the extension numbers.
- 3 To define the number Call Sender uses to call back this user, in the Callback DN box, type a DN (the default is the primary extension DN).
- 4 To let external callers call the directory entry by spelling its name, make sure the Name dialable by external caller check box is checked.
- 5 To record a spoken name for this directory entry's Personal verification, follow the procedure in [“Recording a spoken name for a directory entry” on page 133](#).

Recording a spoken name for a directory entry

Introduction

Record a unique name for the directory entry that identifies the phone when someone is sending a message or composing a distribution list.

Before you begin

Select the SDL to which you want to add users and open its SDL Properties property sheet. You must also follow the procedures in [“Creating a directory entry for the shared distribution list” on page 131](#) and [“Defining the settings for a directory entry” on page 132](#).

Getting there CallPilot System > User Administration > Shared Distribution Lists > File > Properties (New directory entry user button) > Add Directory Entry User > Settings tab

To record a name for a directory entry

- 1 To record a name on behalf of the directory entry, click Record.
Result: The Specify Phoneset dialog box appears.
- 2 In the Enter a phone number in dialable format box, type the phone number of the phoneset you want to use for recording.
- 3 Answer the phoneset when it rings.
Result: The Voice Recorder dialog box appears.
- 4 Click Record.
- 5 Speak a name for the directory entry user into the phoneset.
- 6 Click Stop.
- 7 To review the recorded name, click Play.
- 8 If you are happy with the recording, click Done to return to the Settings tab.
- 9 If you are unhappy with the recording, repeat steps [4](#) through [6](#).

Importing a WAV file for a directory entry

Introduction

Import a file that contains the name identifying a directory entry. Callers and message senders hear the spoken name during call answering and various messaging sessions.

Before you begin

Select the SDL to which you want to add users and opened its SDL Properties property sheet. You must also follow the procedures in [“Creating a directory entry for the shared distribution list” on page 131](#) and [“Defining the settings for a directory entry” on page 132](#).

Getting there CallPilot System > User Administration > Shared Distribution Lists > File > Properties (New directory entry user button) > Add Directory Entry User > Settings tab

To import a WAV file

- 1 To import a WAV file, click Import.
- 2 Select the file that contains a recording of the directory entry's name.
- 3 Click Open.

Viewing a shared distribution list

Introduction

View the contents of an SDL to confirm the users assigned to the list and other settings for the list.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To view a distribution list

- 1 Select a distribution list.
- 2 On the File menu, select Properties.

Result: The SDL Properties window appears.

Viewing or changing a shared distribution list

Introduction

View or change the users and property settings of an SDL.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To view or change an SDL

- 1 Select a distribution list.
- 2 On the File menu, select Properties.
Result: The SDL Properties window appears.
- 3 Follow, as required, the procedures in [“Setting up a shared distribution list” on page 117](#).

Deleting a user from a shared distribution list

Introduction

Delete a user that you no longer want to include in an SDL.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To delete a user from an SDL

- 1 Select the SDL from which you want to delete a user.
- 2 On the File menu, select Properties.
Result: The SDL Properties window appears.
- 3 To delete a user from the current distribution list, click the user in the Distribution list contents box.
- 4 Click Remove to delete the user from the list.
- 5 Click Save.

Deleting a shared distribution list

Introduction

Delete an SDL that you no longer need.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To delete a shared distribution list

- 1 Select an SDL.
- 2 On the File menu, select Delete.
Result: A dialog box appears, asking you to confirm the deletion.
- 3 Click Yes to delete the list.

Printing shared distribution lists

Introduction

Print the contents of an SDL when you want a hard copy of all the settings. You can also print a list of all the SDLs on the system.

Getting there CallPilot System > User Administration > Shared Distribution Lists

To print the contents of a shared distribution list

- 1 Select an SDL.
- 2 On the File menu, select Properties.
- 3 Click Print.

To print a list of all SDLs

- 1 On the File menu, select Print.
- 2 Click OK when the printer settings are correct.

Chapter 6

Performing server backups

In this chapter

Overview	142
Section A: About performing server backups	143
About backing up server data	144
Section B: Working with backup devices	149
About backup devices	150
Adding backup devices to the Backup Devices window	154
Modifying or deleting backup devices	156
Section C: Scheduling server backups	159
About scheduling server backups	160
Opening the Backup Scheduler	163
Scheduling server backups	165
Modifying and deleting scheduled backups	170
Monitoring or canceling backups	171
Section D: Setting up remote disk backups	175
About remote disk backups	176
Planning the configuration	177
Creating a writable share on the remote file server	179
Reconfiguring the backup and restore on the CallPilot server	199
Verifying the network configuration	204
Creating a disk device on the CallPilot server	206
Section E: Restoring your CallPilot system	207
Restoring your CallPilot system from the base hardware	208

Overview

Introduction

This chapter provides information on how to schedule server backups to prevent data loss, and how to restore the CallPilot server after a failure.

- [Section A: “About performing server backups,” on page 143](#), describes the types of predefined backups that are available.
- [Section B: “Working with backup devices,” on page 149](#), describes the backup devices that are provided and recommended, and how to define new backup devices.
- [Section C: “Scheduling server backups,” on page 159](#), describes how to schedule a predefined backup. It also provides information on how to modify or delete a scheduled entry, and how to monitor or cancel a running backup.
- [Section D: “Setting up remote disk backups,” on page 175](#), describes how backups can be performed to a remote disk.
- [Section E: “Restoring your CallPilot system,” on page 207](#), describes how to locate the procedures for restoring the CallPilot server from the base hardware.

Section A: About performing server backups

In this section

[About backing up server data](#)

[144](#)

About backing up server data

Introduction

A server backup lets you save and restore a complete set of system and multimedia data files from your CallPilot server in the event of disk drive failure or corrupted or lost configuration and messaging data. Backups also protect against data loss due to theft or damage caused by natural disasters.

A complete server backup consists of a single backup for each logical disk drive installed on your server. If you want to do a specific backup of user archives, prompt archives, or Application Builder archives, see [Chapter 7, “Archiving and restoring data from archives.”](#)

You can back up files to server tape or to another specified device. Backups are scheduled from the CallPilot Administration Client. They can also be performed immediately using the Tool Launcher on the server.

Perform server backups frequently and at regular intervals to prevent data loss.

Restoring from backups

ATTENTION

Your distributor is responsible for restoring server backups to return the server to the state it was in when the backup was created.

Procedures for reinstalling the CallPilot system and restoring your data are located in Part 5 of the *Installation and Configuration Guide* for your platform.

RAID systems

Backups protect against data loss due to software problems (for example, file system corruption, registry corruption, and failed upgrades), undetected disk errors, double faults, and human error. In addition, backups are useful for migration to a different CallPilot platform. For these reasons, Nortel Networks recommends that periodic backups be done even on servers with RAID. Store the backup tapes separately from the CallPilot server.

Required security level and password

Security

Log on to the CallPilot Administration Client with an administrator user ID.

Password

The CallPilot Backup and Restore service requires the same password as the password used for NGenSys.

If you have changed the Windows NT user account password for NGenSys, see [“To change the CallPilot Backup and Restore service password to match NGenSys” on page 426.](#)

Requirements

To perform a complete server backup, schedule predefined backups to correspond to the number of drives on your server. Before you schedule a predefined backup, ensure that the destination device is listed in the Backup Devices table.

Predefined server backups

When you install CallPilot, two types of predefined server backups are installed on the server—the system backup and the secondary disk backup. These backups are not scheduled to run automatically. You must schedule them using the Backup Scheduler.

To schedule a predefined backup, see [Section C: “Scheduling server backups,” on page 159.](#)

A complete set of server backups consists of

- a system backup
- one secondary disk backup for each additional disk drive on your server (for example E, F)

You can schedule the backups separately; however, you must have a backup of all disks to do a complete restore of the CallPilot server.

System backup

The system backup saves all your data on drives C and D. Schedule a system backup to copy the following items to the specified backup device:

- the database
- Windows NT registry
- Multimedia File System (MMFS) volume 1
- Nortel Networks dynamic data files

Secondary disk backups

The secondary disk backup saves all your data stored on the additional disks on the server. Each disk represents one volume.

Note: On a RAID system, you back up a partition on a mirrored disk pair where two disks represent one volume. For example, if you have four disks, they equal two volumes; therefore, you do two secondary disk backups for the two volumes.

Schedule secondary disk backups to copy the following items to the specified backup device:

- recorded user messages
- greetings
- customized prompts
- Application Builder prompts and applications

Excluded data

Server backups do not save the following software. If a catastrophic failure occurs, you must reinstall this software as part of the complete CallPilot system restore procedure:

- Windows NT 4.0
- CallPilot server software
- CallPilot client software
- Any PEPs applicable to your system

The *Installation and Configuration Guide* for your server describes the complete restore procedures. Your distributor is responsible for data restore procedures from backup for your system.

Backup speed

The speed with which backups are performed depends on the current load on the system and whether the backup device is local.

The following table illustrates the total elapsed time required to perform a backup for various system types and sizes. The Total Backup Elapsed Time (in minutes) includes the time to back up system and user data. For example, the time to back up a 200i system with a 4 Gbyte tape drive, no load, 30 hours of user data, and the system data is 29 minutes.

Total Backup Elapsed Time (in minutes)						
Platform		30 hour	100 hour	200 hour	600 hour	1000 hour
200i	4 Gbyte tape drive, no load	29	60	103		
	4 Gbyte tape drive, with 100% channels busy	40	71	114		
702t	16 Gbyte tape drive, no load	11	18	28	69	110
	16 Gbyte tape drive, 75% channels busy	16	23	33	74	115
1001rp	16 Gbyte tape drive, no load	11	18	28	69	110
	16 Gbyte tape drive, 75% channels busy	16	23	33	74	115

Restore times are comparable to no-load backup times.

Formulating a backup strategy

A well-planned backup strategy minimizes the risk of losing data. When you formulate your strategy, consider the following points:

- Which data is critical to the organization and should be backed up?
- How often does data change?
Periodically, you can back up data that changes infrequently. Back up data that changes constantly more often, especially if it is critical to the organization.
- Who will maintain the backups and do they fully understand their roles? Be sure they know how to label backup media for easy retrieval.
- Determine on-site and off-site locations for backup media. Ensure that only authorized personnel have full access to the sites. Store your backup media in an environment that meets the media manufacturer's storage requirements.

Section B: Working with backup devices

In this section

About backup devices	150
Adding backup devices to the Backup Devices window	154
Modifying or deleting backup devices	156

About backup devices

Introduction

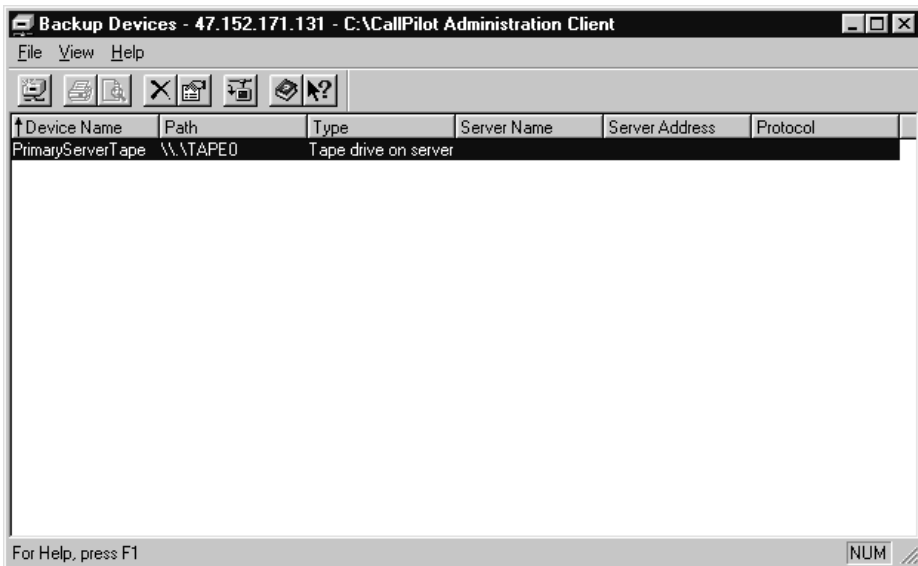
When you schedule a predefined backup, you must specify a destination backup device that is listed in the Backup Devices window.

Some devices are predefined and automatically listed in the Backup Devices window when the CallPilot server software is installed. If the device for the backup that you want to schedule is not listed, add it to the Backup Devices window.

Getting there CallPilot System > System Administration > Server Backup > Backup Devices

The Backup Devices window

The Backup Devices window lists all destination devices for which you can schedule a backup.



To add a backup device to the Backup Devices window, see [“Adding backup devices to the Backup Devices window” on page 154](#).

Predefined devices

The following devices are predefined by the server software. These devices automatically appear in the Backup Devices window if the server is configured to list them.

Note: The PrimaryServerDisk device is no longer available as a backup device. The PrimaryServerDisk represents local disk space that must not be used for server backups because the backed-up data is lost if the disk fails.

PrimaryServerTape

The PrimaryServerTape represents a tape drive located on the server. The PrimaryServerTape is the most common device for backups.

The PrimaryServerTape is always listed in the Backup Devices window. Before scheduling a backup to the PrimaryServerTape, make sure that a tape drive is installed on your CallPilot server.

ATTENTION

Do not change the directory path to the backup device. Changing the path will cause the backup to fail.

Remote disk backups

You can configure the CallPilot server to allow backups to be performed to a remote file server, such as a Windows 95/98 workstation or Windows NT server, rather than a tape drive.

For more information on setting up remote disk backups, see “About remote disk backups” on page 176.

Tape devices

All backup tapes must be specially formatted for server data. When you schedule a backup, you can select Autoformat to format the tape, if necessary, immediately before the scheduled backup runs. This process destroys existing data on the tape.

Overwriting existing data

When you schedule a backup, select **Overwrite** to replace the contents of the tape with the new backup. If you do not select **Overwrite**, the new backup is appended to existing server backup data on the tape.

Note: If you schedule your system backup and your secondary disk backups to run one after the other and intend to use the same tape, select **Overwrite** only on the first backup. If you select **Overwrite** on the subsequent backups, you overwrite the data from the earlier one.

Recommended devices

You can perform backups on remote hard disks, or with the following tape drives:

- Tandberg SLR32 QIC
- Tandberg SLR5
- Tandberg SLR50
- MLR1

Verify that backups are successful

Nortel Networks recommends that you periodically verify that your scheduled backups are completed successfully, with no items skipped. Skipped items on server backups indicate a problem—such backups might not provide sufficient data to restore your system completely in the event of a catastrophic failure.

You can determine the completion status of your most recent backups using the Event Browser on the Administrative Client (see “Using the Event Browser” on page 271). You can filter on event codes 41800 through 41899 to view all recent initiations and completions of backups and restores, as well as other significant backup/restore events.

To see a more extensive history of backup completion status, open the Backup Scheduler on the Administrative Client. This dialog box automatically pops up a scrollable dialog box showing the completion status of all backups performed in the last 90 days. See “Opening the Backup Scheduler” on page 163 for details.

A detailed diagnostic log for each backup completed in the last 90 days is available in the server directory D:\Nortel\Data\Backup\BackupLogs. The logfiles are named for the backup that was done (for example, *SystemBackup*, followed by the date and time the backup was started, with the file extension *log*).

Note: Some messages in this diagnostic log, which appear to be error messages, are in fact normal events that are handled by the Backup/Restore service, and do not necessarily indicate a problem. Your primary indication of backup problems is that the overall completion status is other than *successful* with no items skipped.

Storage and maintenance

Rotate backup tapes regularly and store at least one set of server backups off-site. Do not keep a tape in the tape drive for an extended period of time for the following reasons:

- If the same tape is used for several consecutive backups and the tape becomes damaged, no other backup is available to restore lost data.
- Consistent reuse of the same tape accelerates wear on the tape. You might need to replace tapes earlier than their normal life span.

To prolong the life of your tape heads and ensure the quality of backups, purchase and use head-cleaning kits. Clean tape drives based on the frequency of use. Recommended guidelines for cleaning are provided with most cleaning kits.

Adding backup devices to the Backup Devices window

Introduction

You can only schedule a backup on those devices listed in the Backup Devices window. If the device is not listed, add it to the window before you schedule a backup.

Predefined devices

When the CallPilot server is installed, predefined devices are listed. For more information on these devices, see [“About backup devices” on page 150](#).

Getting there CallPilot System > System Administration > Server Backup > Backup Devices

To add a backup device

- 1 In the Backup Devices window, click File > New.

Result: The New Backup Device Properties window appears.



- 2 Specify a name for the device.

Note: The limit is 240 characters.

- 3 Based on whether the device is local or remote disk space, enter the path of a disk directory as follows:
 - For local disk directories, enter the absolute pathname (for example, E:\TEMP).

ATTENTION

If you define a local disk device, do not use it for server backups. A local disk device does not provide adequate protection against disasters. Also, the local disk device can quickly become full and might cause unrecoverable data corruption.

- For remote disk directories, enter the universal naming convention path (for example, \\SERVER1\BACKUPDATA).
- 4 Specify the type of backup device.
 - 5 Click Save.

Modifying or deleting backup devices

Introduction

This section describes how to

- modify a backup device
- view details about a backup device
- delete a backup device from the Backup Devices window

Getting there CallPilot System > System Administration > Server Backup > Backup Devices

To modify a backup device

- 1 In the Backup Devices window, click File > Properties.

Result: The Backup Device Properties window appears.



The screenshot shows a dialog box titled "PrimaryServerTape - Backup Device Properties". It has two tabs: "General" (selected) and "Details". The "General" tab contains the following fields:

- Name:** A text box containing "PrimaryServerTape".
- Path:** A text box containing "\\TAPE0".
- Type:** A dropdown menu with "Tape" selected.
- Remote Tape:** A section containing three fields:
 - Server Name:** A dropdown menu.
 - Server Address:** A text box.
 - Protocol:** A text box.

At the bottom of the dialog box are three buttons: "Save", "Cancel", and "Help".

- 2 Modify any of the following fields:
 - Name
 - Path
 - Type

- 3 Select Save to save changes to the Backup Device properties.

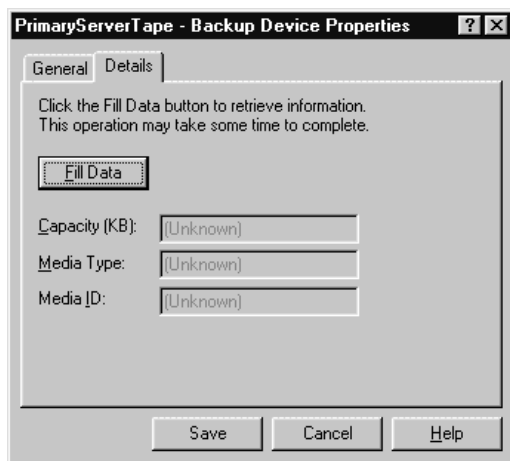
To view details for a backup device

- 1 In the Backup Devices window, click File > Properties.

Result: The Backup Device Properties window appears.

- 2 Click the Details tab.

Result: The Details page appears.



To delete a backup device

- 1 In the Backup Devices window, select the backup device that you want to delete.
- 2 Click X in the Backup Devices window toolbar.

Section C: Scheduling server backups

In this section

About scheduling server backups	160
Opening the Backup Scheduler	163
Scheduling server backups	165
Modifying and deleting scheduled backups	170
Monitoring or canceling backups	171

About scheduling server backups

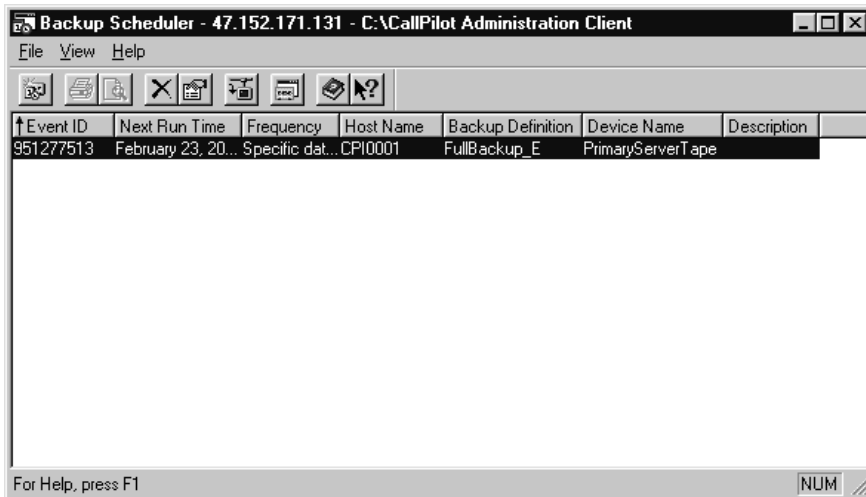
Introduction

After the CallPilot server is installed and operational, schedule the appropriate server backups to run using the Backup Scheduler.

Log on to the CallPilot Administration Client as an administrator.

The Backup Scheduler

When you schedule a backup, it appears in the Backup Scheduler.



When backups should run

Schedule backups to run at the following times:

- before and after major system operations take place, such as an upgrade or the application of PEPs
- after you make any major modifications, such as the addition of a large number of users or customized prompts

- at regular intervals during normal operation, according to the criticality of your message data

Even though running a backup at peak hours has only a minimal impact on response time, try to run backups at off-peak hours whenever possible.

Note: If you do administrative tasks while a backup is in progress, that work might be lost if the backup is used to do a restore.

What scheduling involves

To schedule a backup, open the Backup Scheduler to gain access to the Event Properties window. In this window, name the backup and select the destination device and the type of backup. You must also do the following steps:

Specify the dates and times of the backup

Schedule a backup to run once on a specific day and time, or at regular intervals (daily, weekly, monthly, yearly).

Specify a maximum wait interval (optional)

The maximum wait interval is the period of time during which a scheduled backup attempts to run if it cannot start on time. Specify the maximum wait interval to reduce the risk of missing a backup due to conflicts between the backup and other events, such as the MMFS audit.

Notes:

- Set the maximum wait interval so that if the backup must wait the maximum time, it still completes within the off-peak period.
- If a backup cannot start at the specified time, an Information Event is generated. If the backup cannot start within the specified maximum wait interval, a minor alarm is generated. See Part 2, “Monitoring the CallPilot system,” for information on how to interpret alarms.

ATTENTION

You must check to ensure that the backup was completed with no errors before you can assume that the backup is usable. Check the Alarm Monitor for errors.

ATTENTION

You can schedule backups to run online while calls are being serviced. (Restores are performed offline.) However, because backups compete with services for system resources, schedule backups to run during off-peak hours. To determine the peak call processing periods, see [Chapter 2, “Configuring operational measurements.”](#) for more information.

Do not schedule backups during the MMFS audit hour (3:00 a.m. to 4:00 a.m., server time); they will not start while the MMFS audit is in progress.

Opening the Backup Scheduler

Introduction

View the schedule for a description of a scheduled backup from the Backup Scheduler. This window also lets you access the Event Properties window in which you schedule predefined backups.

Administrative privileges required

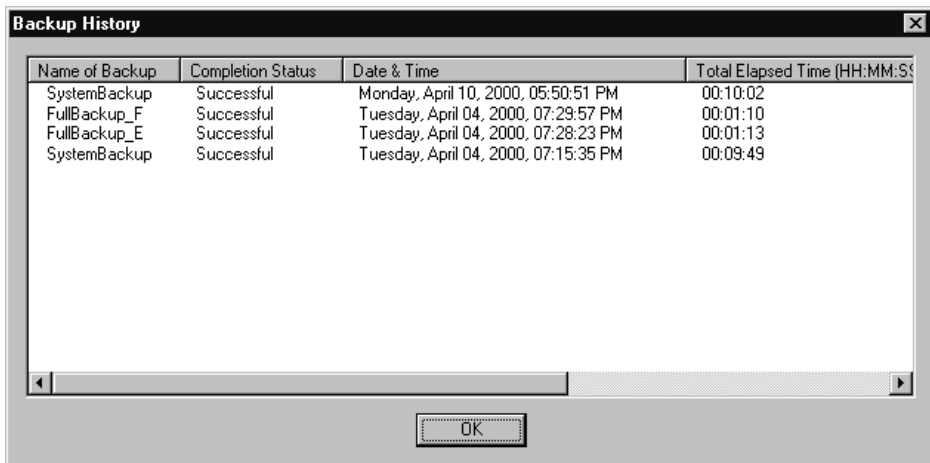
Log on as an administrator.

Getting there CallPilot System > System Administration > Server Backup > Backup Scheduler

To open the Backup Scheduler

- 1 From Server Backup, double-click Backup Scheduler.

Result: The Backup History dialog box appears.



- 2 Use the left and right scroll bars to display additional columns showing
 - total size of the backup in kilobytes

- the name of the destination device
- the Primary (CallPilot) error code
- the Extended (Windows) error code

(See the CallPilot *Maintenance and Diagnostic Guide* for a complete list of CallPilot and Windows error codes.)

The table below gives brief descriptions of the more common error codes.

Primary error	Secondary error	Explanation
41807	1112	There is no tape in the tape drive.
41808	19	The tape in the drive is write-protected.
41825 or 41829	0	The tape is blank or in a foreign format – use AutoFormat.
41827	1	The incorrect tape driver is installed, or the tape medium is not compatible with the tape drive.
41827	23	Received a CRC error reading or writing – clean the drive or use a fresh tape.
41828	1100	The backup did not fit onto the tape – use a fresh tape or specify overwrite.

- 3 Click OK to close the Backup History dialog box.

Scheduling server backups

Introduction

When you schedule a backup, it appears in the Backup Scheduler. To schedule a backup, open the Backup Scheduler to gain access to the Event Properties window.

ATTENTION

Backups compete with services for system resources. Schedule backups to run during off-peak periods and outside MMFS audit hours (3:00 a.m. to 4:00 a.m., server time).

Before you begin

Ensure that the destination device to which the backup is performed is listed in the Backup Devices window. See [“Adding backup devices to the Backup Devices window” on page 154](#).

Types of backups

The following server backup types are available:

Backup type	Description
SystemBackup	performs a backup of the system drives C and D
FullBackup_E	performs a backup of the secondary drive E
FullBackup_F	performs a backup of the secondary drive F

Autoformatting tapes

All backup tapes must be specially formatted for CallPilot server backup data. When you schedule a backup, select Autoformat to format the tape immediately before the scheduled backup runs. This process destroys existing data on the tape the first time you autoformat for CallPilot.

The system can detect when a tape is already formatted for CallPilot, and it does not autoformat again.

Overwriting existing data

When you schedule a backup, select Overwrite to replace the contents of the tape with the new backup. If you do not select Overwrite, the new backup appends to existing backup data on the tape.

Note: If you schedule your system backup and your secondary disk backups at different times, but intend to use the same tape, do not select Overwrite on the second backup, or you overwrite the data from your first backup.

Getting there CallPilot System > System Administration > Server Backup > Backup Scheduler

To schedule a backup

- 1 From the Backup Scheduler, click File > New Schedule.

Result: The Event Properties window appears.

The screenshot shows the 'Event Properties' dialog box with the 'Schedule' tab selected. The dialog has three tabs: 'General', 'Schedule', and 'Others'. The 'Schedule' tab contains the following fields and options:

- Event ID:** 951277513
- Host Name:** CP10001
- Ownership:**
 - Tag:** Backup_NGen
 - Owner:** sysadmin
 - Customer ID:** 1
- Main:**
 - Device Name:** PrimaryServerTape (dropdown menu)
 - Backup Definition:** FullBackup_E (dropdown menu)
- Submission:**
 - Date:** February 22, 2000
 - Time:** 10:45:13 PM
- Additional options:**
 - ☐ Autoformat
 - ☐ Overwrite

At the bottom of the dialog are three buttons: 'Save', 'Cancel', and 'Help'.

- 2 Select the destination device in the Device Name box.
- 3 Select the type of backup in the Backup Definition box.
- 4 Select Autoformat to format the tape for CallPilot automatically before the scheduled backup runs.

Note: You cannot perform a successful backup on an unformatted tape.

- 5 Select Overwrite if you want the backup to overwrite existing data on the device.

Note: If you are scheduling backups to run one after the other, and you intend to use the same tape, select Overwrite only on the first backup. If you select Overwrite on the subsequent backup, you overwrite the data from the first one.

- 6 Click the Schedule tab.

Result: The Schedule tab appears.

The screenshot shows the 'Event Properties' dialog box with the 'Schedule' tab selected. The 'Specific date(s)' dropdown is open, showing a list of months and days. The 'Start' time is set to 6:37 PM. The 'Maximum wait time' is set to 00:15. There are 'Clear' and 'Invert' buttons for both the date selection and the wait time. At the bottom are 'Save', 'Cancel', and 'Help' buttons.

Month	Day
<input type="checkbox"/> January	<input type="checkbox"/> 1
<input type="checkbox"/> February	<input type="checkbox"/> 2
<input type="checkbox"/> March	<input type="checkbox"/> 3
<input type="checkbox"/> April	<input type="checkbox"/> 4
<input type="checkbox"/> May	<input type="checkbox"/> 5
<input checked="" type="checkbox"/> June	<input type="checkbox"/> 6
<input type="checkbox"/> July	<input type="checkbox"/> 7
<input type="checkbox"/> August	<input type="checkbox"/> 8
<input type="checkbox"/> September	<input type="checkbox"/> 9
<input type="checkbox"/> October	<input type="checkbox"/> 10
<input type="checkbox"/> November	<input type="checkbox"/> 11
<input type="checkbox"/> December	<input type="checkbox"/> 12

Day	Day	Day
<input type="checkbox"/> 13	<input type="checkbox"/> 14	<input type="checkbox"/> 15
<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18
<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21
<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24
<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27
<input type="checkbox"/> 28	<input type="checkbox"/> 29	<input type="checkbox"/> 30
<input type="checkbox"/> 31		

Start: 6 : 37 PM

Maximum wait time: HH:MM 00 : 15

Clear Clear

Invert Invert

Save Cancel Help

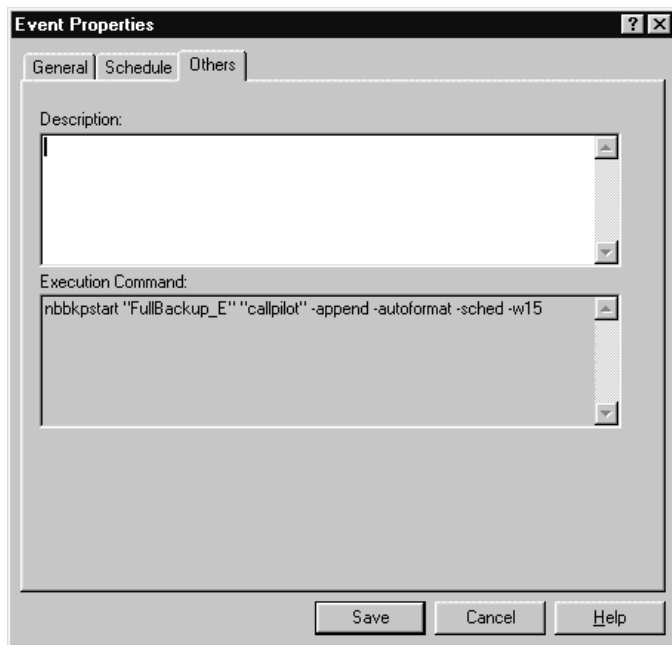
- 7 Select the day or dates on which the backup is going to run.

Tip: Click the drop-down arrow to access daily, weekly, monthly, yearly, or specific dates schedule selections.

- 8 Select the time for the backup to run.
- 9 Select the maximum wait time.

- 10 Click the Others tab.

Result: The Others tab appears.



- 11 Enter any explanatory details about the backup.

- 12 Click Save.

Result: The system schedules the backup and adds it to the Backup Scheduler.

Modifying and deleting scheduled backups

Introduction

Modify details of a scheduled backup using the Event Properties window. You can also delete backups from this window.

Getting there CallPilot System > System Administration > Server Backup > Backup Scheduler

To modify a scheduled backup

- 1 Double-click the backup to be modified in the Backup Scheduler.

Result: The Event Properties window appears.

- 2 Modify details in the General tab.
- 3 Click Schedule.
- 4 Modify details in the Schedule tab.
- 5 Click Other.
- 6 Modify details in the Others tab.
- 7 Click Save.

Result: The system modifies the backup and the changes appear in Backup Scheduler.

To delete a scheduled backup

- 1 From Backup Scheduler, select the scheduled backup you want to delete.
- 2 From the File menu, select Delete.

Monitoring or canceling backups

Introduction

Monitor the status of a running backup using the Backup Status window. This window appears on-screen when a scheduled backup runs.

Current status

View the current status to see if any files were skipped or copied in error during the backup.

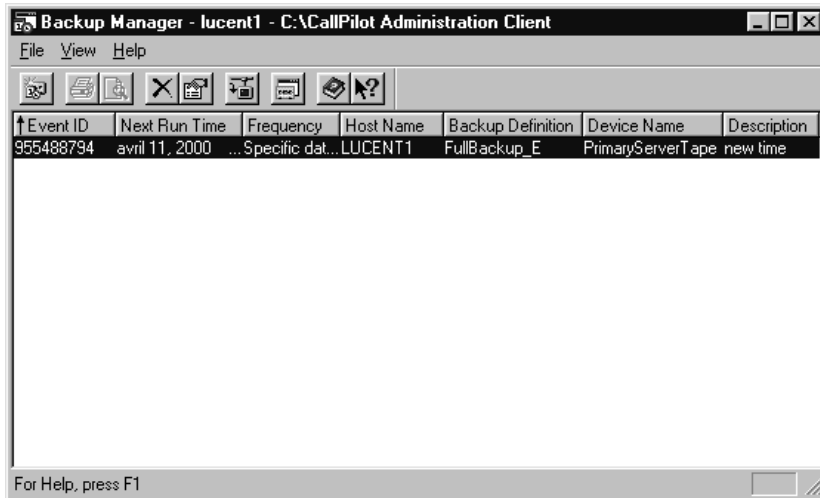
If any files did not copy successfully, a minor alarm is generated. Obtain the Event ID from the alarm in the Alarms Monitor for information.

If an error occurred during the backup, you might not be able to restore data from that backup medium. Repeat the backup until it has no errors.

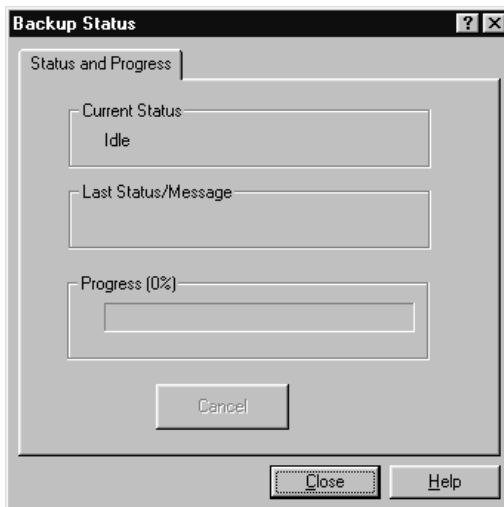
Getting there CallPilot Administration Client > System Administration > Server Backup > Backup Manager

To view the current status

- 1 On the Backup Manager dialog box, click the current backup to highlight it, and then click View > View Backup Status.



Result: The Backup Status dialog box appears.



To cancel a running backup

Click Cancel on the Backup Status window to stop a running backup.

Any data that is successfully written to the backup device before the backup is canceled is unusable.

- The unusable data from the previous backup remains on the tape, and the data for the new backup is recorded following the unusable data.
- If a subsequent backup is appended to this tape, it is written to the tape following the unusable data.

Section D: Setting up remote disk backups

In this section

About remote disk backups	176
Planning the configuration	177
Creating a writable share on the remote file server	179
Reconfiguring the backup and restore on the CallPilot server	199
Verifying the network configuration	204
Creating a disk device on the CallPilot server	206

About remote disk backups

Introduction

You can configure the network to allow backups to be performed to a remote disk, such as a Windows 95/98 workstation or Windows NT server, rather than a tape drive.

To set up remote disk backup to other server types, contact the appropriate network administrator for assistance.

Steps required

Complete the following steps to set up and perform remote disk backups to a suitable workstation or server:

1. Plan the configuration (on page [177](#)).
2. Create a writable share on the remote file server (on page [179](#)).
3. Reconfigure the Backup/Restore service on the CallPilot Server (on page [199](#)).
4. Verify the Network Configuration (on page [204](#)).
5. Create a Disk Device on the CallPilot Server (on page [206](#)).
6. Schedule a backup or archive to the Remote Disk Device (on page [159](#)).

Planning the configuration

Introduction

Before you can configure the network to allow backups to be performed to a remote disk, plan the configuration.

As part of the initial planning you must

- identify an appropriate workstation or file server to store your CallPilot backup
- ensure there is sufficient disk space on the target server to hold the planned backups
- determine the mode of security access and user verification that is required for the Backup and Restore service to access the remote disk backup directory

Supported workstation or file server

The target workstation or file server for the remote disk backup must support long file names. Windows NT, Windows 95/98, and other servers that support file storage from a Windows PC are all acceptable.

Required disk space

The target workstation or file server must have sufficient disk space available for the types of backups that are to be placed on the remote backup server.

To back up the entire system requires approximately 250 Mbytes, plus 10 Mbytes for each hour of storage on the system. For example, a 30-hour system requires 550 Mbytes of disk space to accommodate a backup of the entire system, while a 1000-hour system requires 10.25 Gbytes.

CallPilot selective archives can vary widely, depending on the number of items selected for the archive, but usually require much less disk space than a full set of system backups.

Security and user verification

You must configure the target workstation or server so that the Backup/Restore service is granted access to the remote disk backup directory. The access control method you choose is determined by the configuration of the remote disk backup server and by the security requirements of your location.

There are two types of control methods, as follows:

- **Share-level access control** Allows access for all users. The backup directory is not password-protected.
- **User-level access control** Access is restricted to specific users. You must configure the backup/restore service as a user in the domain of the remote disk backup server.

If your remote disk backup directory is on a Windows 95/98 workstation, you can choose either share-level or user-level access control. On Windows NT remote disk backup servers, you must use user-level access control.

If your remote backup directory is on a FAT partition, you control access to the network share, since you cannot assign access permissions to the directory itself.

If your remote backup directory is on an NTFS partition, there is no need to control access to the network share. You can apply the permissions directly to the backup directory. This is preferable since it controls both local and remote access.

Creating a writable share on the remote file server

Introduction

Create a shared directory on the server that stores the CallPilot backup data. Do not use this directory for any other purpose. Regularly back up data to removable media using the site backup procedures in use at your location.

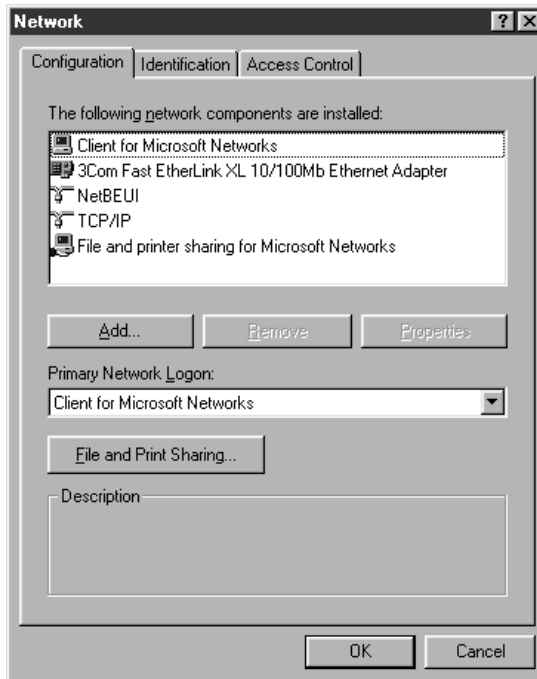
Based on the selected target network drive, set up the writable share as outlined in the appropriate procedure:

- For Windows 95/98, see [“To create a writable share on the Windows 95/98 remote file server” on page 180.](#)
- For Windows NT, see [“To create a writable share on a Windows NT remote file server” on page 188.](#)

Note: For Windows 95/98 workstations, ensure that the share you create is writable and *not* password-protected.

To create a writable share on the Windows 95/98 remote file server

- 1 Select Start > Settings > Control Panel.
- 2 Double-click Network to display the Network window.
- 3 On the Configuration tab, click File and Print Sharing... near the bottom of the window.

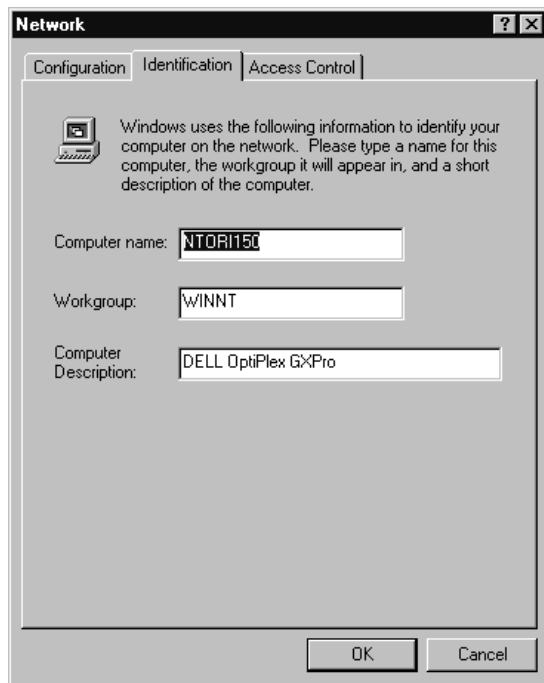


- 4 In the File and Print Sharing window, check the box labeled I want to be able to give others access to my files. This configures the computer to permit file sharing.



- 5 Click OK to exit the File and Print Sharing dialog box.

- 6 Select the Identification tab and note the Computer name assigned to this computer. You need this information when you set up the CallPilot server.

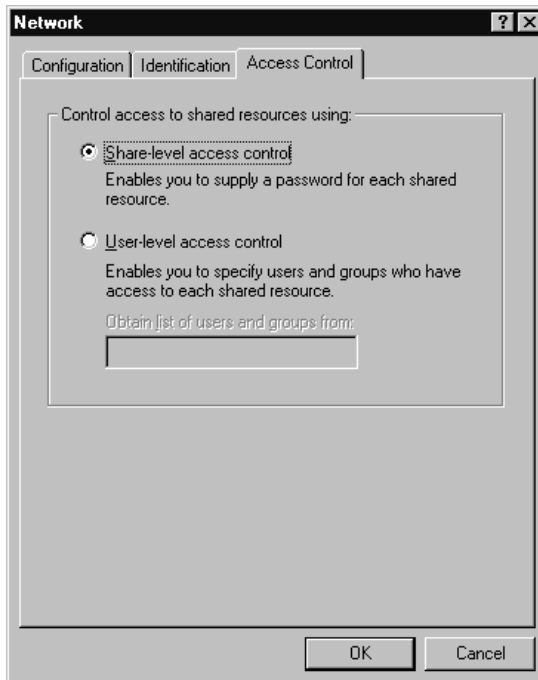


- 7 Determine the level of access to be assigned to the writable share, and proceed with the appropriate step, as outlined below:
 - For Share-level access control, continue with step 8.
 - For User-level access control, continue with step 15.

For Share-level access control:

- 8 Select Share-level access control on the Access Control tab.

Note: Although Share-level access control is easier to set up, it is less secure than User-level access control.

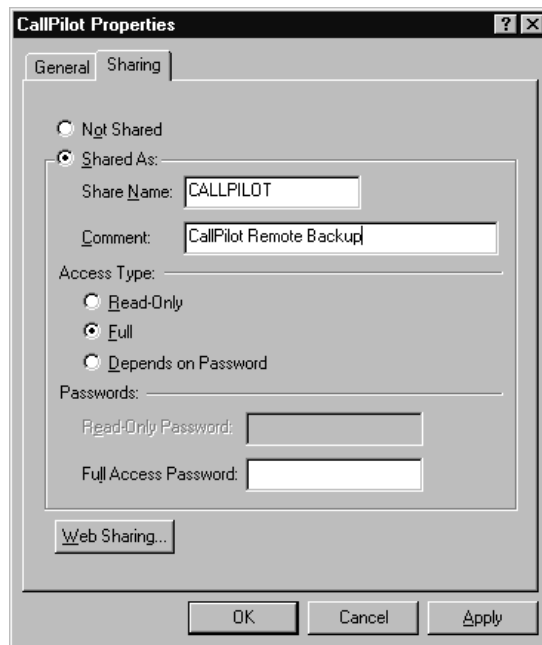


- 9 Click OK to exit the Network window.

- 10** If you have made changes, you are prompted to restart the computer. If you enabled file sharing, the system might require you to insert your Windows 95/98 CD so that some files can be copied to your system.



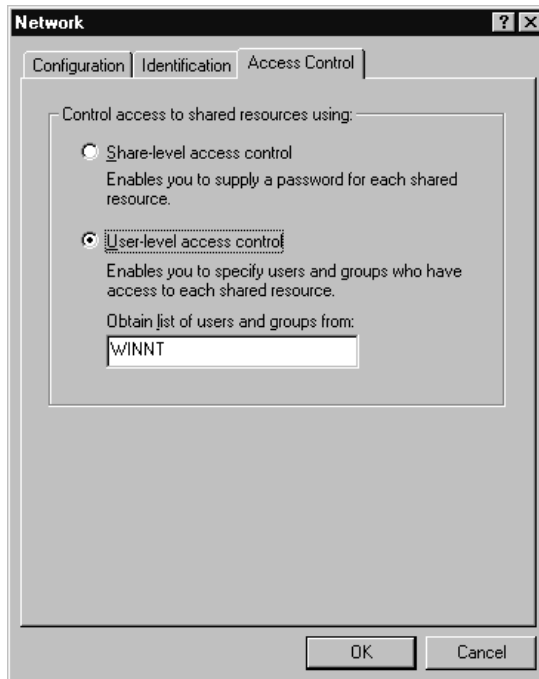
- 11** Click Yes to restart the computer and put the new setting into effect.
- 12** Create a shared directory for the remote disk backups, as follows:
- Open Windows Explorer and navigate to the drive you have chosen for remote disk backups. Highlight the drive name.
 - Select File > New > Folder to create a new folder on that drive (for example, D:\CallPilot Backups).
 - Right-click the new folder and select the Sharing tab on the Properties dialog box.



- d. Click Shared As, and type in a Share Name and optional comment. The share name must be 1 to 12 characters in length, using letters, digits, and underscore only. If you want to make this share invisible to workstation browsers, use a dollar sign as the last character.
 - e. Click Full from the Access Type group to assign full access permission to the remote backup directory. *Do not* type in a password.
- 13 Click OK to set the access permissions and create the share.
- 14 Refer to "What's next?" after step 23 to continue with the setup of the remote backup server.

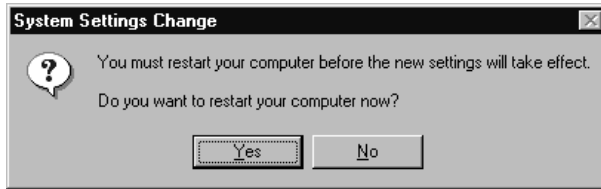
For User-level access control:

- 15 Select User-level access control on the Access Control tab. Make a note of the Windows NT domain from which you can obtain a list of users and groups.



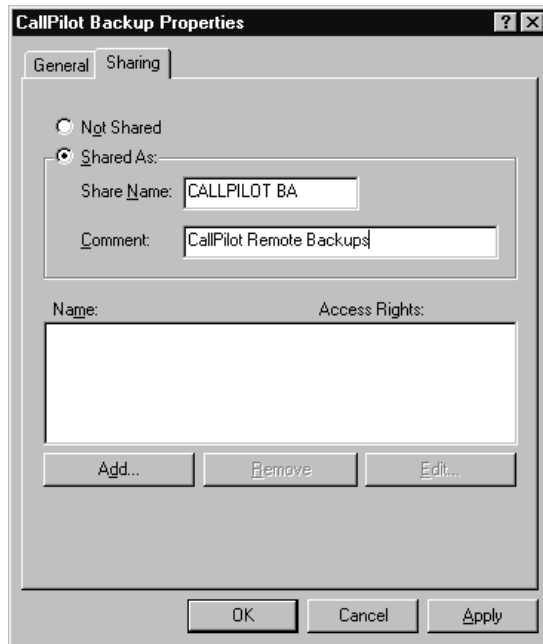
- 16 Click OK to exit the Network window.

- 17** If you have made changes, you are prompted to restart the computer. If you enabled file sharing, the system might require you to insert your Windows 95/98 CD so that some files can be copied to your system.



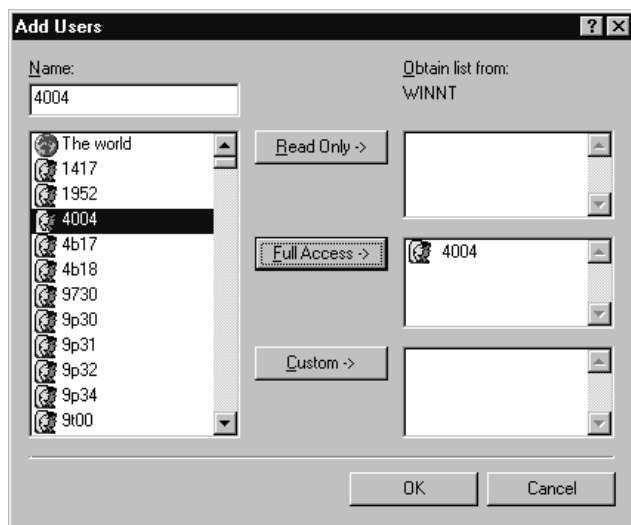
- 18** Click Yes to restart the computer and put the new setting into effect.
- 19** Have the network administrator create a user ID (for example, CP_Backup) on the domain where your workstation is obtaining its list of users and groups. Use this user ID for remote disk backups only. Ensure this user ID is set up with the right to "access this computer from the network." No other rights are required.
- 20** Create a shared directory for the remote disk backups, as follows:
- a.** Open Windows Explorer and navigate to the drive you have chosen for remote disk backups. Highlight the drive name.
 - b.** Select File > New > Folder to create a new folder on that drive (for example, D:\CallPilot Backups).
 - c.** Right-click the new folder and select the Sharing tab on the Properties dialog box.

- d. On the Properties dialog box, select Shared As, and type in a Share Name and optional comment. The share name must be 1 to 12 characters in length, using letters, digits, and underscore only. If you want to make this share invisible to workstation browsers, use a dollar sign as the last character.



- 21 Assign user-level access permissions to the remote backup directory, as follows:
 - a. Click Add... on the Properties window to display the Add Users dialog box.
 - b. Select the user ID that you created in step 19 from the list on the left side.

- c. Click Full Access to move this user into the middle list on the right side.



- 22 Click OK on the Add Users dialog box to set the access permissions.
- 23 Click OK on the Properties dialog box to create the share.

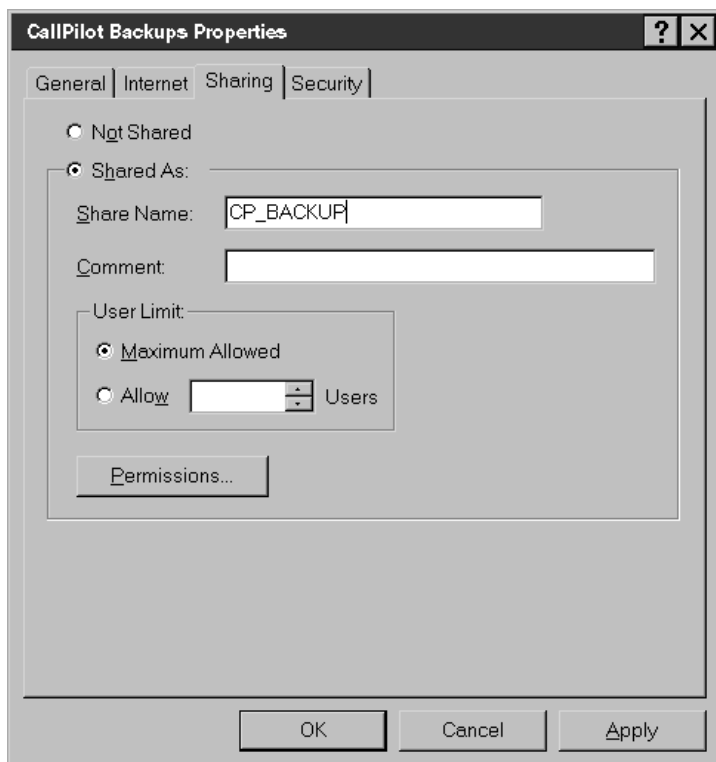
What's next?

See [“Reconfiguring the backup and restore on the CallPilot server” on page 199](#).

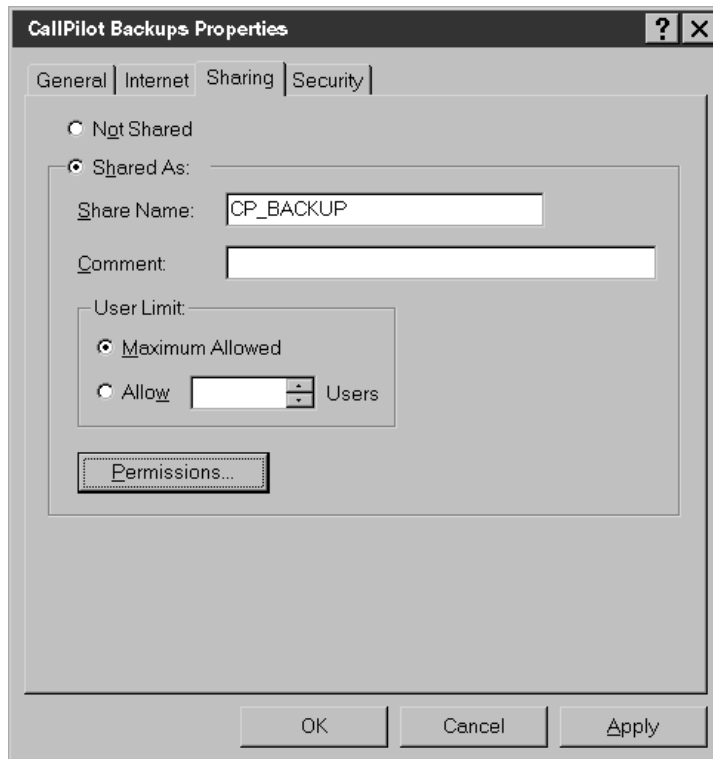
To create a writable share on a Windows NT remote file server

- 1** On your remote file server, create a local user to be used for remote disk backups only. This user ID (for example, CP_Backup) must have the right to “access this computer from the network.” No other rights are required.
- 2** Create a shared directory for the remote disk backups, as follows:
 - a.** Open Windows Explorer and navigate to the drive you have chosen for remote disk backups. Highlight the drive name.
 - b.** Select File > New > Folder to create a new folder on the selected drive (for example, D:\CallPilot Backups).
 - c.** Right-click the new folder and open the Properties window. Select the Sharing tab.

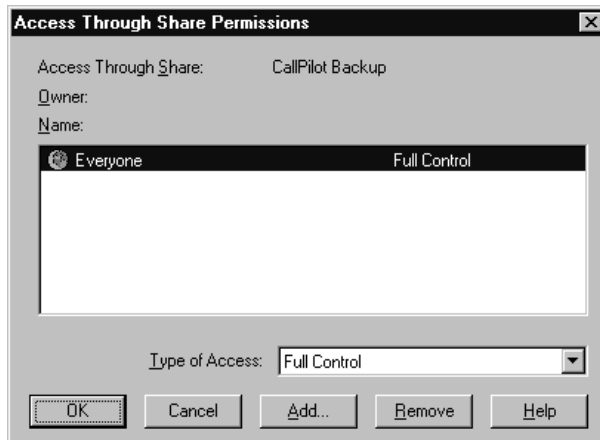
- d. On the Sharing tab, click Shared As, type a name in the Share Name box, and enter a comment in the optional Comment box. The share name must be 1 to 12 characters in length, using letters, digits, and underscore only. If you want to make this share invisible to workstation browsers, use a dollar sign as the last character.



- 3 Determine whether the remote directory is on a FAT partition or NTFS partition, and proceed with the appropriate step, as outlined below:
 - For FAT partitions, continue with step 4.
 - For NTFS partitions, continue with step 5.
- 4 For FAT partitions, assign access permissions to the remote backup directory share, as follows:
 - a. On the Sharing tab, click Permissions to assign access permissions to this share.



- b. On the Access Through Share Permissions dialog box, select Everyone and click Remove.



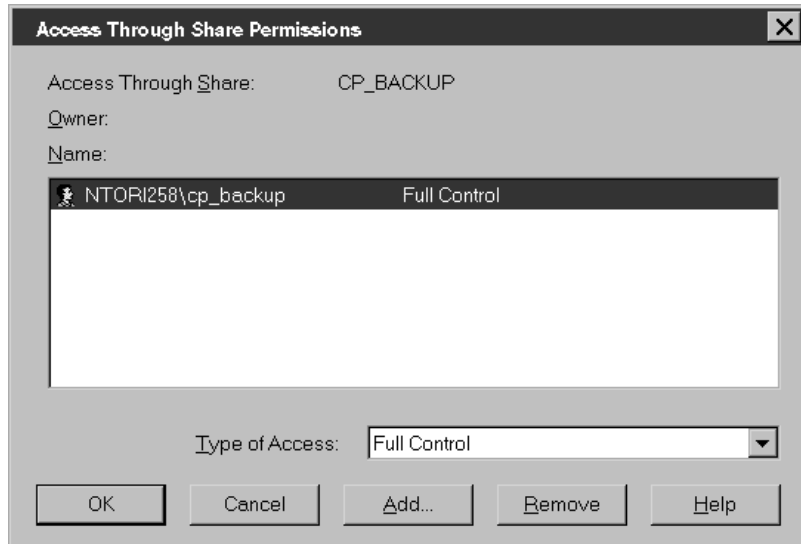
- c. Click Add to display the Add Users and Groups dialog box to add specific permissions.

- d. On the Add Users and Groups dialog box, click Show Users, and select the user ID you created in step 1 from the Names list.



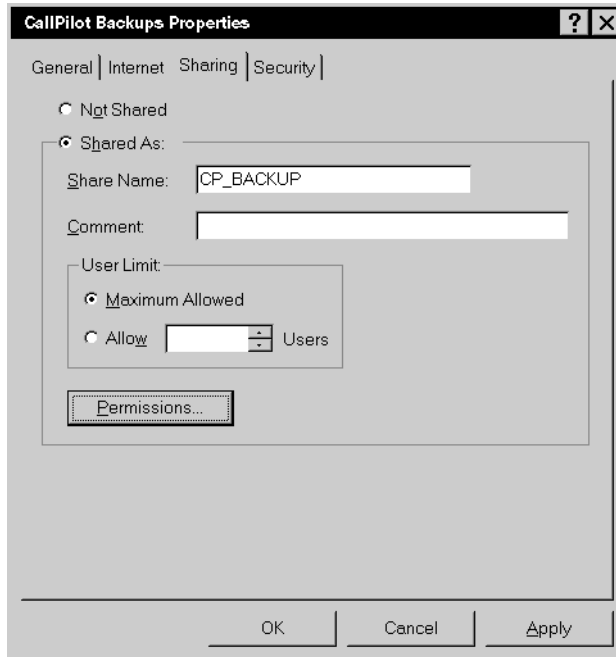
- e. Click Add to move this user into the Add Names text box.
- f. Select Full Control from the Type of Access combo box at the bottom of the window, and click OK.

- g. On the Access Through Share Permissions dialog box, verify that the new user ID appears with Full Control, and then click OK.

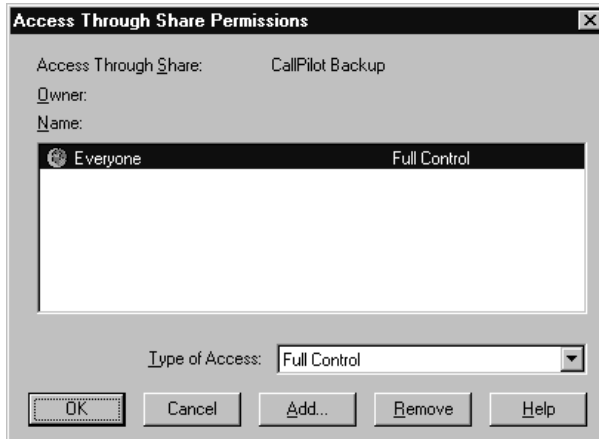


- h. Click OK on the Properties dialog box to create the share. If the name is longer than eight characters, you might get a warning about accessibility from MS-DOS workstations. You can ignore this warning.

- 5 Assign access permissions to the remote backup directory NTFS partition, as follows:
 - a. On the CallPilot Backups Properties window, select the Sharing tab and click Permissions.



- b. On the Access Through Share Permissions dialog box, ensure the permissions are set to the default Everyone - Full Control.

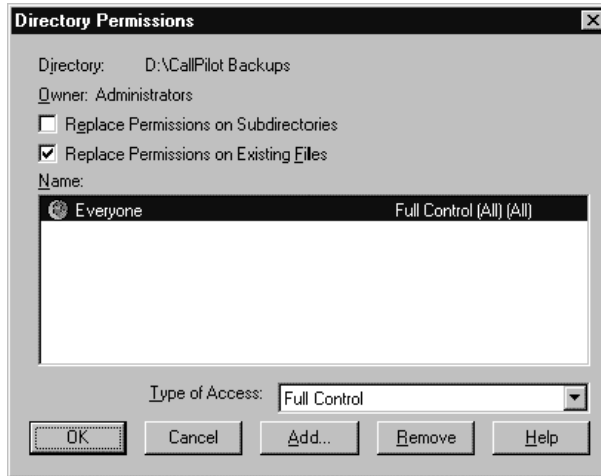


- c. On the CallPilot Backups Properties window, select the Security tab.

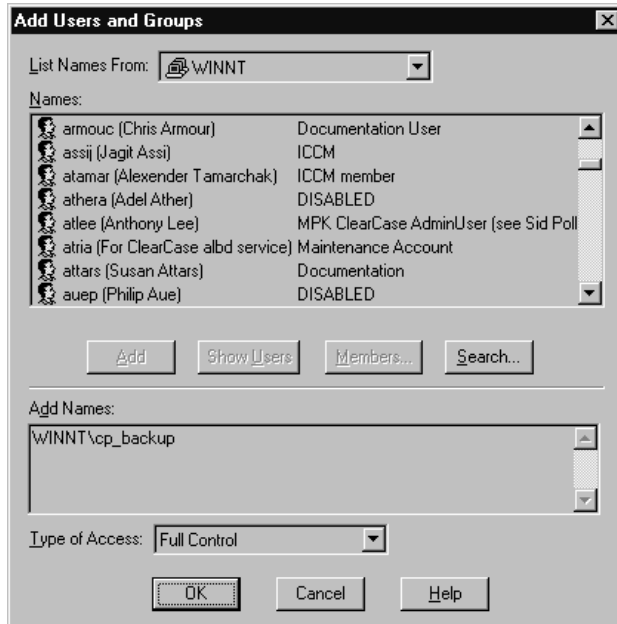


- d. Click Permissions to display the Directory Permissions dialog box. On the Directory Permissions dialog box, the default permissions are inherited from the parent directory.

- e. Select each item in the Name list box, and click Remove until the list box is empty.



- f. Click Add to display the Add Users and Groups dialog box to add specific permissions.



- g.** On the Add Users and Groups dialog box, click Show Users, and select the user ID you created in step 1 from the Names list.
- h.** Click Add to move this user into the Add Names text box.
- i.** Select Full Control from the combo box at the bottom of the dialog box, and click OK.
- j.** On the Directory Permissions dialog box, verify that the user ID appears with Full Control beside it, and then click OK.
- k.** Click OK on the CallPilot Backups Properties window to create the share. If the name is longer than eight characters, you might get a warning about accessibility from MS-DOS workstations. You can ignore this warning.

What's next?

See [“Reconfiguring the backup and restore on the CallPilot server” on page 199](#).

Reconfiguring the backup and restore on the CallPilot server

Introduction

Once you have set up the shared directory on the remote backup server and assigned the appropriate network access permissions, configure the CallPilot server to access that shared directory.

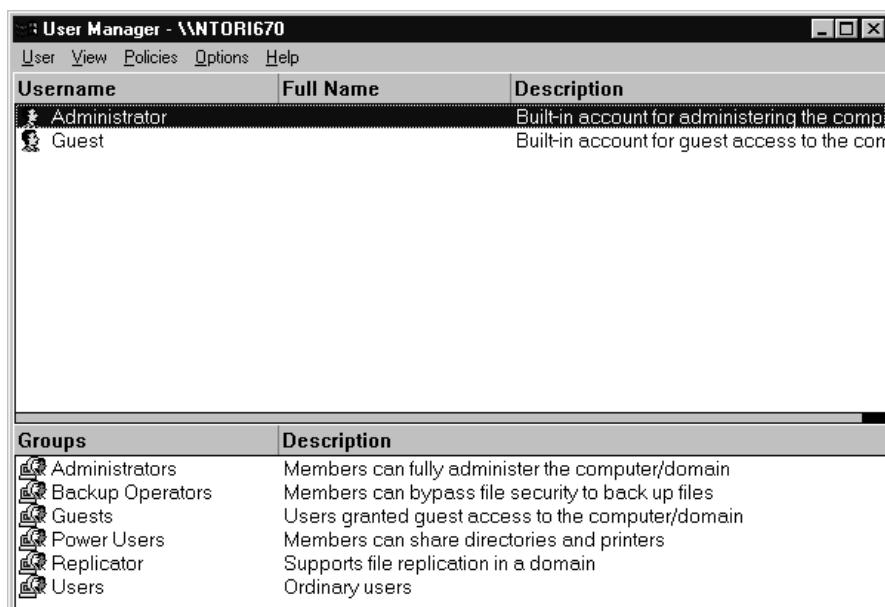
ATTENTION

This procedure is not required for backups that are being performed on a Windows 95/98 workstation using share-level access control. For those configurations, continue with the next procedure, [“To verify the network configuration” on page 204](#).

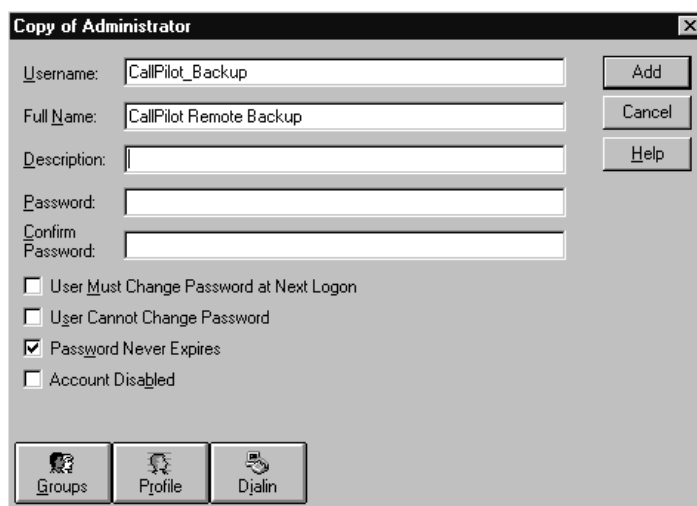
To reconfigure the backup and restore on the CallPilot server

- 1 Log on to the CallPilot server using a user ID with administrative access.
- 2 From the Start menu, select Programs > Administrative Tools (Common) > User Manager for Domains.

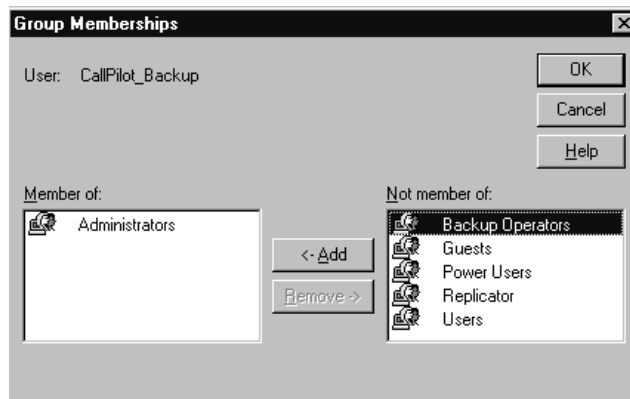
- 3 In User Manager, select the Administrator user ID from the list.



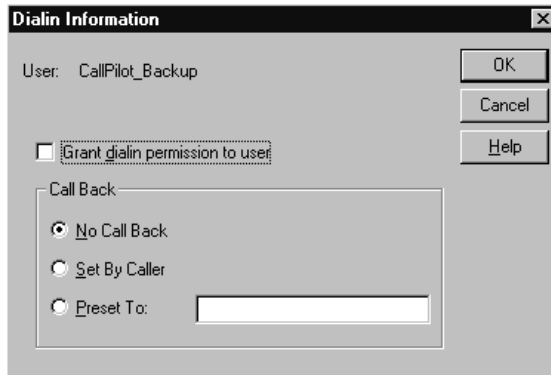
- 4 Select User > Copy from the menu bar. The Copy of Administrator dialog box appears.



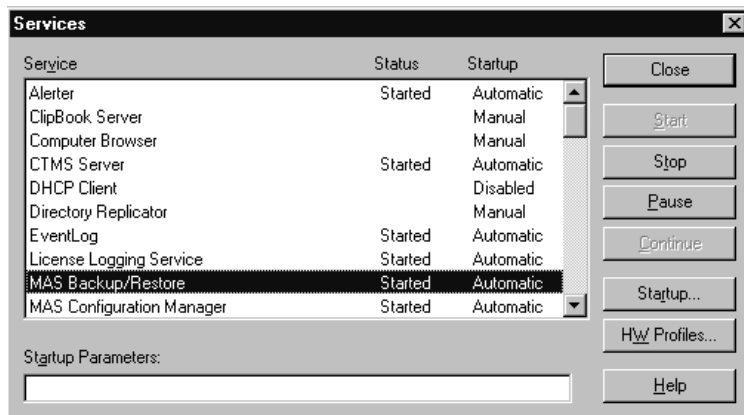
- 5 On the Copy of Administrator dialog box, in the Username field, enter the user name you created on the remote network domain for performing remote backups. Enter the Full Name and Description, using any characters that you want.
- 6 Enter the password for the user that you created for the remote network domain into the Password and Confirm Password fields. Verify that the settings for the following fields in the middle of the dialog box are correct:
 - User Must Change Password at Next Logon - Unchecked
 - User Cannot Change Password - Unchecked
 - Password Never Expires - Checked
 - Account Disabled - Unchecked
- 7 On the Copy of Administrator dialog box, click Groups, and verify that the new user is a member of the Administrators group.



- 8 On the Copy of Administrator dialog box, click Dialin, and verify that the new user does not have dial-in access.

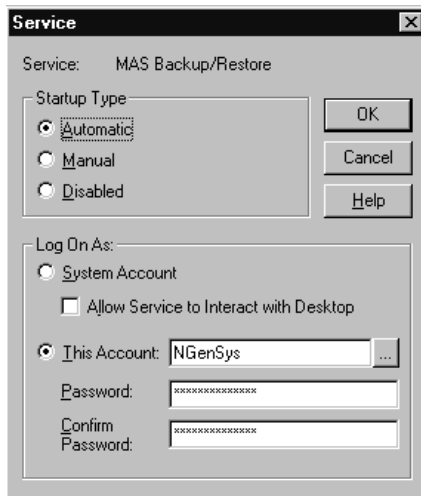


- 9 Click OK to return to the Copy of Administrator window.
- 10 Click Add to add the new user. The name now appears in the main list.
- 11 Exit the User Manager.
- 12 From the Start Menu, select Settings > Control Panel, and launch the Services applet.



- 13 Select the Backup/Restore service and click Start.

- 14** In the Log On As frame, select This Account.



- 15** Type in the user ID and password for the user you just created, and then click OK.
- 16** Stop, and then Start the Backup/Restore service on the Services window so that the new user ID and password settings take effect.
- 17** Close the Services applet and the Control Panel.

What's next?

Verify the network configuration.

Verifying the network configuration

Introduction

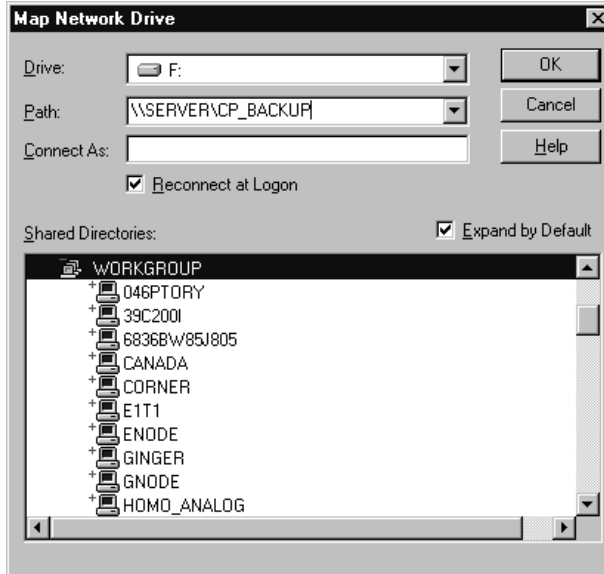
Verify the network access from the CallPilot server to the remote backup server to ensure that the remote access has been established correctly.

To verify the network configuration

- 1 Log on to the CallPilot server, using the user ID that you created in the previous procedure, [“Reconfiguring the backup and restore on the CallPilot server” on page 199.](#)

Note: If you are performing backups to a Windows 95/98 workstation using share-level access control, log on as Administrator or any other server account known to you.

- 2 Open Windows Explorer and select Tools > Map Network Drive to display the Map Network Drive combo box.



- 3 Select an unused drive letter in the Drive combo box.

- 4 In the path combo box, type in the path to the remote backup directory. Use \\SERVER\CP_BACKUP, where SERVER is the computer name of the remote backup server, and CP_BACKUP is the share name of the directory you created.
- 5 Leave the Connect As text box blank, uncheck the Reconnect at Logon check box, and then click OK.
Note: If you get an error message, verify that the computer name matches the remote file server's computer name exactly. Also, verify that the share name matches the remote file server's share name (not the directory name) exactly.
- 6 Try to copy a file into the root directory of the newly mapped drive.
- 7 Verify that the file has been created correctly, and that you can subsequently delete the file. If this cannot be done, verify the following information:
 - The user ID and password on the CallPilot server exactly match the user ID and password on the remote backup server's domain.
 - Full access permissions for the user ID have been assigned to the remote share or directory.
- 8 Select Tools > Disconnect Network Drive to delete the drive mapping you created.
- 9 Log off the CallPilot Server.

What's next?

Create a disk device on the CallPilot server.

Creating a disk device on the CallPilot server

Introduction

Create a backup device that can be used to direct backups to the remote disk directory.

Getting there CallPilot System > System Administration > Server Backup > Backup Devices

To create a disk device on the CallPilot Server

- 1 From the Backup Devices window, select File > New from the menu bar to create a new backup device.

Result: The New Backup Device Properties window appears.

- 2 In the Name field, enter a descriptive name.
- 3 In the Path field, enter the network path to the remote backup directory. For example, \\SERVER\CP_BACKUP, where SERVER is the computer name of the remote backup server and CP_BACKUP is the share name (not the directory name) of the shared directory that you created.

The name of the new backup device that was created in this step will appear in the dialog boxes that specify the name of the target device to which the backup or archive is directed.

Note: Do not use mapped drive letters to specify the path to the remote backup directory. These drive mappings are in effect only if a real user is logged on to the CallPilot server. If no user is logged on to the server, the drive mappings do not exist.

- 4 Click Save.

The CallPilot Administration Client can now be used to schedule backups or selective archives to the remote disk directory. See [Section C: “Scheduling server backups,” on page 159](#) for information on scheduling system backups or archives.

Section E: Restoring your CallPilot system

In this section

[Restoring your CallPilot system from the base hardware](#)

[208](#)

Restoring your CallPilot system from the base hardware

Introduction

In the case of a complete system failure, you might need to rebuild your CallPilot system from the base hardware up.

When you receive your server from the factory, some software, such as the operating system and the CallPilot server software, is already installed. The installation instructions in the *Installation and Configuration Guide* specific to your server begin where the factory installation stops.

However, in the case of a complete system failure, call your CallPilot distributor. Your *Installation and Configuration Guide* also contains the information you need to reinstall a complete system from scratch. Your CallPilot distributor and your system administrator can use the information in the *Installation and Configuration Guide* to rebuild your system.

Chapter 7

Archiving and restoring data from archives

In this chapter

Overview	211
Section A: About archives	213
What are archives?	214
Kinds of archive	216
Why restore data from archives	217
Section B: Performing archives	219
Opening Archive Manager	220
Setting up an Application Builder archive	221
Updating an Application Builder archive	222
Removing applications from an Application Builder archive	223
Setting up a User archive	224
Updating a User archive	225
Removing users from a User archive	227
Setting up a Prompt archive	228
Setting a schedule for an archive	229
Performing an immediate archive	231
Section C: Restoring data from archives	233
Opening Restore Manager	234
Changing the archive device	236
Restoring Application Builder applications from an archive	237
Restoring user data	239

[Selecting the languages of prompts to be restored](#)

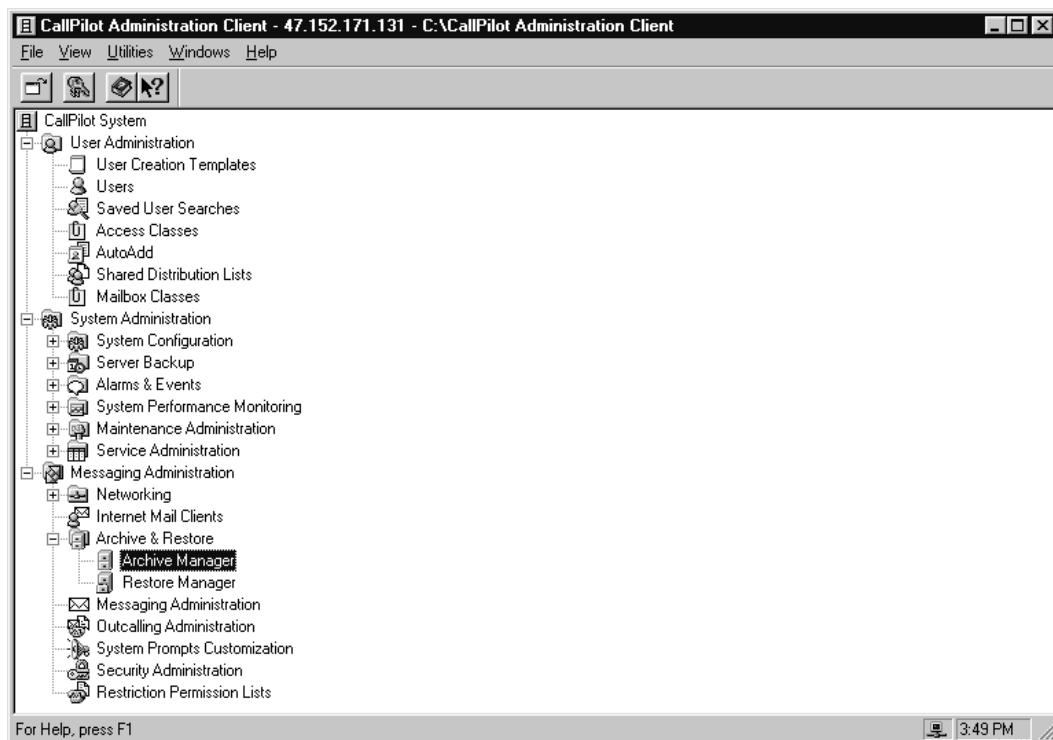
[241](#)

Overview

Introduction

This chapter explains how to create archives so that you can save frequently changing CallPilot information while online. It also explains how to restore selected information from earlier archives.

You access your Archive and Restore tools from the CallPilot Administration Client, as shown below.



Section A: About archives

In this section

What are archives?	214
Kinds of archive	216
Why restore data from archives	217

What are archives?

Introduction

Archives are copies of multimedia files from CallPilot. Archives specifically back up Application Builder applications, personal user data (such as greeting, messages, and personal distribution list), and customized voice prompts.

You can immediately save archives or schedule them while your system is still online. If you want to recover the data and restore it to the system, you can select the specific information you want to restore.

How an archive differs from a system backup

Both backup and archive copy data to tape or to disk. This stored data is not used unless it must be restored.

Archives

You can selectively restore data from an archive without taking the CallPilot system out of service. If you restore one or more messages from an archive, they are added to the messages currently in the user's mailbox. Any user custom commands or the user's personal verification cannot be restored from an archive. Archive does not save switch-related setup, operational measurement data, event logs, alarms, system security settings, the networking setup, or queues of undelivered and time-delayed messages.

Archive and selective restore lets you

- support recovery from inadvertent deletions of a user's messages or mailbox, personal distribution lists (PDLs), customized prompts, and Application Builder applications
- port Application Builder applications from another system

System backups

After any necessary hardware repairs, your distributor uses the backup data to restore a complete set of system and multimedia data files (server only) in the event of disk drive failure or corrupted or lost configuration and messaging data. Backups also protect your system against data loss due to theft or natural disasters.

You can back up files to server tape or to another specified device. Backups can be scheduled or performed immediately from the CallPilot Administration Client.

You can restore these files to return the server to the state it was in when the backup was created. You cannot selectively restore data using backup.

Perform system backups frequently and at regular intervals to prevent data loss.

Frequency

As the administrator, you must evaluate whether to create archives or to do system backups and how frequently you do so, based on the value of the different kinds of data to your business.

Kinds of archive

Introduction

Archive Manager enables you to archive constantly changing information on your system while you are online. There are three kinds of archive:

- user archives
- prompt archives
- Application Builder archives

User archives

User archives let you select the users you want to save. The user data that is saved includes

- voice and fax messages
- user mailbox greetings (external, internal, and temporary)
- PDLs
- the actual configuration of a user

Note: This release of CallPilot does not support archiving of user-defined speech-recognition commands. If a user's mailbox is lost and recovered from an archive, the user must redefine his or her custom speech-recognition commands.

Prompt archives

Prompt archives include any customized prompts (which are default system prompts that were substituted by the customer in System Prompt Customization). You must save all the customized prompts. The default system prompts are saved when you perform system backups.

Application Builder applications archives

Application Builder archives enable you to select and save any applications created using Application Builder, whether the application is in service or not.

Why restore data from archives

Introduction

Restore Manager lets you quickly restore data that is accidentally deleted by a mailbox user or an administrator.

Users

Users sometimes accidentally delete user messages, PDLs, and user greetings. The user archive lets you save the data belonging to users, and then choose the data you want to restore. For instance, you can restore a specific voice message.

Prompts

If you delete a customized prompt, the system automatically returns to the default system prompt. To recover the customized prompt, restore it from a prompt archive. You must restore prompts in each language on your system.

Application Builder applications

Application Builder applications are easy to restore from an archive.

You can also copy complex applications from one site to another. Install the applications by “restoring” them at another site. The second site must be running the same or a newer version of the CallPilot server and CallPilot software as the archiving site.

Section B: Performing archives

In this section

<u>Opening Archive Manager</u>	<u>220</u>
<u>Setting up an Application Builder archive</u>	<u>221</u>
<u>Updating an Application Builder archive</u>	<u>222</u>
<u>Removing applications from an Application Builder archive</u>	<u>223</u>
<u>Setting up a User archive</u>	<u>224</u>
<u>Updating a User archive</u>	<u>225</u>
<u>Removing users from a User archive</u>	<u>227</u>
<u>Setting up a Prompt archive</u>	<u>228</u>
<u>Setting a schedule for an archive</u>	<u>229</u>
<u>Performing an immediate archive</u>	<u>231</u>

Opening Archive Manager

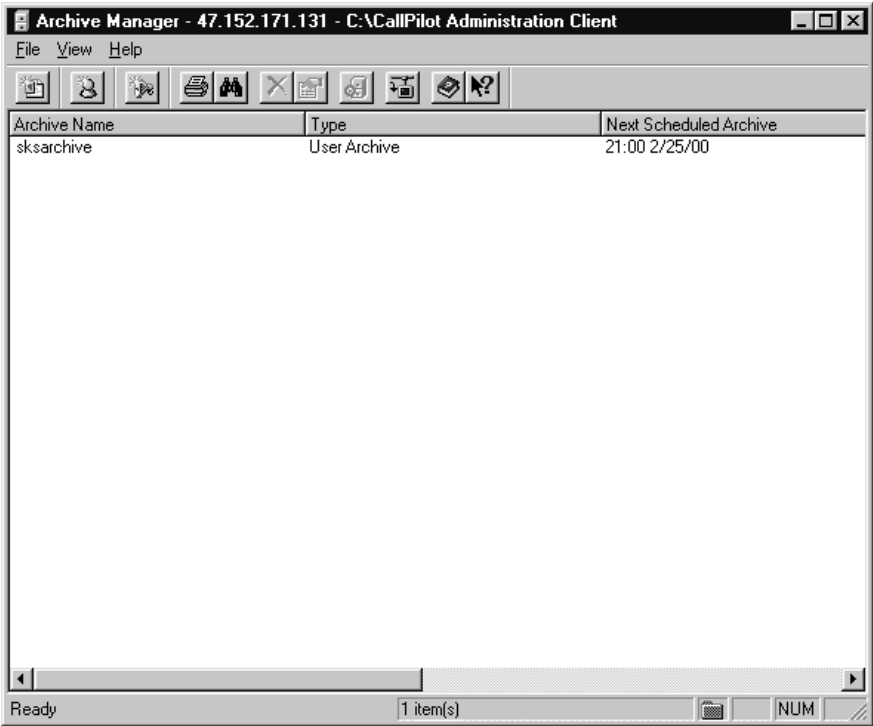
Introduction

Use Archive Manager to back up your Application Builder applications, personal data files, and customized voice prompts.

Getting there CallPilot System > Messaging Administration > Archive & Restore

To open Archive Manager

Double-click Archive Manager.



Setting up an Application Builder archive

Introduction

Set up an archive to back up the Application Builder applications of your choice.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Archive Manager

To set up an Application Builder applications archive

- 1 On the File menu, select New, and then select Application Builder Archive.

Result: The New Application Builder Archive dialog box appears.

- 2 In the Archive Name box, type a name for the applications you are archiving.
- 3 In the Comments box, type additional information about the archive.
- 4 In the Applications List box, click the application you want to include in the archive.
Hold down Ctrl or Shift to select multiple applications.
- 5 Click Add.
- 6 Click Set Schedule to define when the system performs the archive. Follow the procedure in ["Setting a schedule for an archive" on page 229](#).
- 7 After completing the schedule, click Save.

Updating an Application Builder archive

Introduction

Update an Application Builder archive to include new applications that you created since the archive was defined.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Archive Manager

To update an Application Builder application archive

- 1 Find the AppBundle archive in the list of scheduled archives, and double-click it.

Result: Result: The Application Builder Archive window appears

On the left side, the Applications List contains all the applications that are defined on your server that are not included in the archive.

- 2 In the Applications List, click the application you want to add to the archive.
- 3 Hold Ctrl or Shift to select multiple applications.
- 4 Click Add to add the selected applications to the archive, or click Add All to add all the applications in the Application List to the archive.
- 5 Click Save to save the updated archive.

At this point, you may get an Errors dialog containing a list of applications that were originally included in the archive, but that have been deleted from the server. You should remove these applications from the archive by switching back to the Application Builder Archive dialog and removing the non-existent users from the archive.

Tip: Double-clicking on a message in the Errors Dialog will scroll the Application to be backed up list in the Application Builder Archive dialog to a point at or near the application that needs to be removed from the archive.

- 6 When all non-existent applications have been removed from the archive, close the Errors dialog, and press Save again.

Removing applications from an Application Builder archive

Introduction

Remove any Application Builder applications from the list of applications in the archive.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Archive Manager > Application Builder Archive

To remove applications from an Application Builder archive

- 1 In the Applications to be backed up list, hold down Ctrl and select the applications you want to remove from the archive.
- 2 Click Remove.
- 3 Click Save.

Setting up a User archive

Introduction

Set up an archive to back up only the users that you select.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Archive Manager

To set up a User archive

- 1 On the File menu, select New, and then select User Archive.
Result: The New User Archive window appears.
- 2 In the Archive Name box, type a name for the user data you are archiving.
- 3 In the Comments box, type additional information about the archive.
- 4 Click Filter Users to generate a list of mailboxes for the Mailbox Users list.
Select users from the generated list to include in the User archive. If you do not specify search criteria for users, the default user list shows all the users in the system.
Tip: You can perform multiple searches in case you need to specify different search criteria.
- 5 In the Mailbox Users list, click the user you want to include in the archive.
Hold down Ctrl or Shift to select multiple users.
- 6 Click Add.
- 7 Click Set Schedule. Follow the procedure in [“Setting a schedule for an archive” on page 229](#).
- 8 After completing the schedule, click Save.

Updating a User archive

Introduction

Update a User archive to include new users you created since the archive was defined.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Archive Manager

To update a User archive

- 1 Find the User archive in the list of scheduled archives, and double-click it.

Result: The User Archive window appears.

- 2 Click Filter Users to generate a list of mailboxes for the Mailbox Users list.

The generated list will not include any users that are already included in the archive. This step may take some time, depending on how many users there are on your server.

- 3 Select users from the generated Mailbox Users list to be added to the archive.

Note: If you do not specify search criteria for users, the default user list shows all the users in the system that are currently not included in the archive.

Tip: You can perform multiples searches if you need to specify different search criteria.

- 4 In the Mailbox Users list, click the user you want to add to the archive.
- 5 Hold Ctrl or Shift to select multiple users.
- 6 Click Add to add the selected users to the archive, or click Add All to add all the users in the Mailbox Users list to the archive.
- 7 Click Save to save the updated archive.

Note: At this point, you may get an Errors dialog box containing a list of users that were originally included in the archive, but that have been deleted from the server.

- 8 Remove these users from the archive by switching back to the User Archive dialog and removing the deleted users from the archive.

Tip: Double-clicking on a message in the Errors dialog box will scroll the Archive Contents list in the Archive Users dialog box to a point at or near the user that must be removed from the archive.

- 9 When all deleted users have been removed from the archive, close the Errors dialog box, and press Save again.

Removing users from a User archive

Introduction

Remove users that you no longer want to include in a User archive.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Archive Manager > New User Archive

To remove users from a User archive

- 1 In the Archive contents list, select the users you want to remove. Hold down Ctrl or Shift to select multiple users.
- 2 Click Remove.
- 3 Click Save.

Setting up a Prompt archive

Introduction

Set up an archive to back up only the customized system prompts created in System Prompt Customization.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Archive Manager

To set up a Prompt archive

- 1 On the File menu, select New, and then select Prompt Archive.
Result: The New Prompt Archive window appears.
- 2 In the Archive Name box, type a name for the prompts you are archiving.
- 3 In the Comments box, type additional information to describe the archive.
- 4 Click Set Schedule. Follow the procedure in [“Setting a schedule for an archive” on page 229](#).
- 5 After completing the schedule, click Save.

See also

For more detailed information about customized prompts, see “Configuring Basic Messaging Options” in the *CallPilot Administrator’s Guide*.

Setting a schedule for an archive

Introduction

Set the frequency and specific times for the system to perform the selective archive that you have chosen.

Note: An archive does not necessarily require a schedule. You can create an archive to use for immediate archiving.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Archive Manager

To set a schedule for an archive

- 1 Double-click the name of the archive that you want to schedule.
Result: The User Archive window appears.
- 2 Click Set Schedule.
Result: The Set Archive Schedule dialog box appears.
- 3 From the Frequency list, select how often the system creates selective archives. Your selection determines which other scheduling boxes can be configured.
- 4 From the Month list, select a month.
- 5 From the Date Of Month list, select a date.
- 6 From the Day Of Week list, select the day.
- 7 From the Start Time list, select the time.
- 8 To define the maximum amount of time the system waits to perform an archive if the backup device is busy, from the Maximum extension period list, select a length of time.
- 9 To define the device to which the archive is saved, from the unlabeled Device list, select the device.
- 10 If the archive saves to disk, go to step [12](#).

11 If the archive saves to tape, choose one of the following actions:

Action	make sure the
To erase the previous archive data on the tape	Overwrite check box is checked.
To format the tape	Auto format check box is checked.

12 Click OK.

Note: The schedule is saved only when you save the archive itself.

Performing an immediate archive

Introduction

Instead of scheduling an archive to run in the future, you can run an existing archive to save vital and current data immediately.

Before you begin

You must have an existing archive in which to save the data.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Archive Manager

To perform an immediate archive

- 1 Select an archive.
- 2 On the File menu, select Archive Now.

Section C: Restoring data from archives

In this section

Opening Restore Manager	234
Changing the archive device	236
Restoring Application Builder applications from an archive	237
Restoring user data	239
Selecting the languages of prompts to be restored	241

Opening Restore Manager

Introduction

Use Restore Manager to restore your archived data.

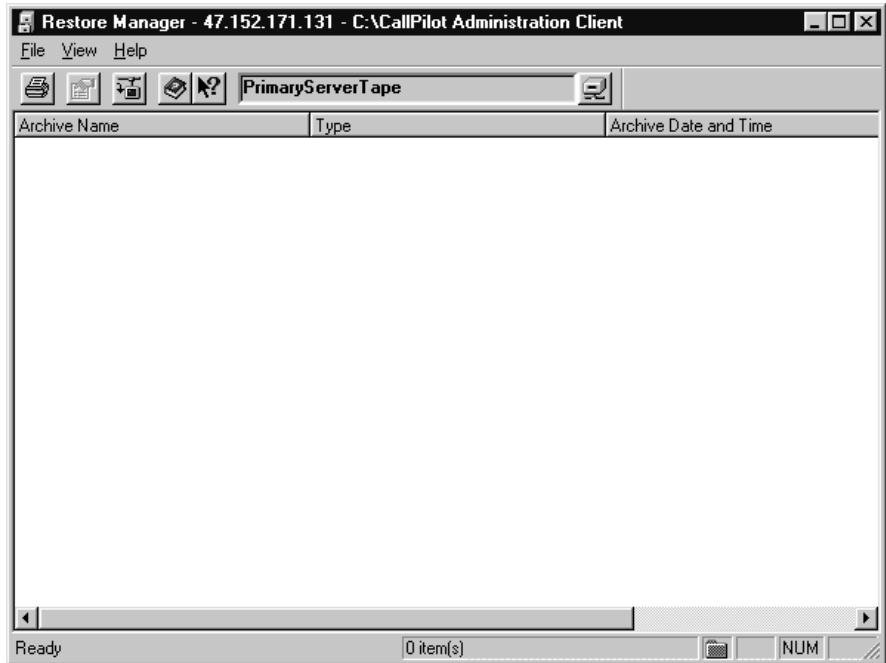
Getting there CallPilot System > Messaging Administration > Archive & Restore

To open Restore Manager

- 1 Double-click Restore Manager.
Result: The Restore Device dialog box and the Restore Manager window appear.
- 2 In the Restore Device dialog box, select the device name that contains your archive.

- 3 Click OK.

Result: The Restore Device dialog box closes and you can work with the Restore Manager.



Changing the archive device

Introduction

Select the device on which an archive is saved. You must select from a list of devices that are defined in the Backup and Restore program.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Restore Manager

To change the archive device

- 1 In the File menu, select Change Device.
- 2 From the list of archive devices, select the device that contains your archive.
- 3 Click Open.

Result: The device containing your archive appears.

Restoring Application Builder applications from an archive

Introduction

Restore selected Application Builder applications from an archive back onto your system.

ATTENTION

If there is a working version of the application you want to restore on your system, you must put the working version out of service. Then open and save the restored application in Application Builder and put the restored application into service.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Restore Manager

Before you begin

Select the archive device that contains the archive you want to restore.

To restore Application Builder applications

- 1 If the Restore Device dialog box opens, select the archive device that contains the Application Builder archive you want to restore.
- 2 In Restore Manager, click the Application Builder archive you want to restore in part or in its entirety.
- 3 On the File menu, click Open.

Result: The Restore Application Builder dialog box appears.

- 4 In the tree view of Application Builder applications in the archive, make sure only those applications that you want to restore are checked.

- 5** To stop the restoration of applications that have the same name or ID as applications currently on your system, make sure Do not restore is selected.
- 6** To restore applications that have the same name or ID as applications currently on your system, and to erase the application on the system, make sure Overwrite with archive copy is selected.
- 7** To restore applications that have the same name and ID as applications currently on your system and to rename the applications that are being restored, make sure Restore with new name and ID is selected.
- 8** To restore the applications to the same volume on the server on which they were previously located, make sure Restore to original volumes is selected.
- 9** To specify which volume applications are restored, make sure Restore to is selected, and select the volume number from the list.
- 10** Click Restore.

Restoring user data

Introduction

Select the user data, such as user messages, greetings, or PDLs, from an archive to restore on your system.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Restore Manager

Before you begin

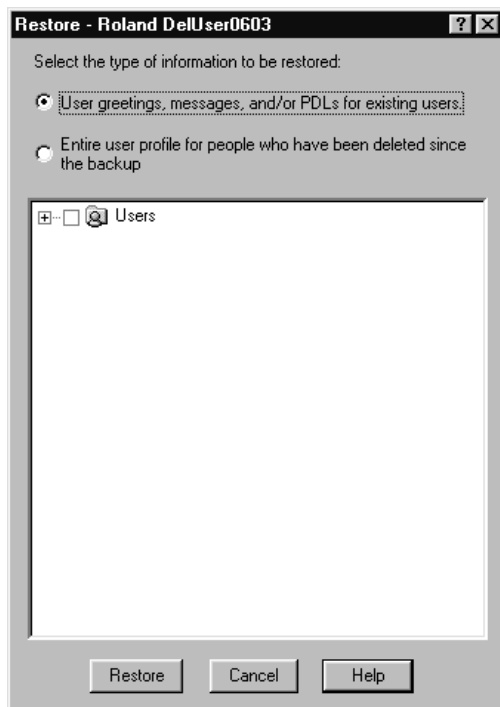
Select the archive device that contains the archives you want to restore.

To restore user data

- 1 If the Restore Device dialog box opens, select the archive device that contains the User Archive you want to restore.
Note: If you are restoring files from the current archive, avoid this dialog box by making sure the Always open with the selected device check box is checked.
- 2 In Restore Manager, select a User Archive.

- 3 On the File menu, click Open.

Result: The Restore Users dialog box appears.



- 4 Select the type of information that you want to restore. Choose from one of the following options:
 - a. User greetings, messages, and/or PDLs for existing users
 - b. Entire user profile for people who have been deleted since the backup
- 5 For existing users, in the tree view, make sure only the user data that you want to restore is checked.
- 6 For users in the list of deleted users, check the user whose entire profile you want to restore.
- 7 Click Restore.

Selecting the languages of prompts to be restored

Introduction

Select the language of the customized system prompts to restore on your system.

Getting there CallPilot System > Messaging Administration > Archive & Restore > Restore Manager

Before you begin

Select the archive device that contains the archives you want to restore.

To select the language of the customized prompts that are restored

- 1 If the Restore Device dialog box opens, select the archive device that contains the Prompt archive you want to restore.

Note: If you are restoring files from the current archive, avoid this dialog box by making sure the Always open with this archive device check box is checked.

- 2 In Restore Manager, select a prompt archive.
- 3 On the File menu, click Open.

Result: The Restore Prompts dialog box appears.

- 4 In the list of prompt languages, make sure only the languages that you want to restore are checked.
- 5 Click Restore.

Part 2

Monitoring the CallPilot system

In this part

Chapter 8: Introduction to monitoring CallPilot	245
Chapter 9: Viewing and filtering server events	261
Chapter 10: Viewing and filtering client PC events	309
Chapter 11: Monitoring the server	315
Chapter 12: Managing channels	343
Chapter 13: Troubleshooting	377

Chapter 8

Introduction to monitoring CallPilot

In this chapter

<u>Alarms and events</u>	<u>246</u>
<u>Disk space usage</u>	<u>249</u>
<u>Server performance</u>	<u>252</u>
<u>Hardware problems</u>	<u>253</u>
<u>Channel state</u>	<u>255</u>
<u>Reports</u>	<u>257</u>

Alarms and events

What are events and alarms

Event

An event is a significant occurrence in the system that requires user notification. Some events warn users of serious problems, such as hardware failure or software errors. Other events inform users of normal occurrences, such as password expiry messages and logon notifications. Events are recorded by the server log as they are generated. They can be viewed or printed at a later time.

Alarm

An alarm is a system notification that lets you know a potential or real problem has occurred. An alarm is automatically generated whenever an event with a default severity of Critical, Major, or Minor has occurred.

Working with events and alarms

Three programs let you work with events and alarms:

- The Event Preferences window lets you customize events by changing their default severity or by throttling.
- The Event Browser lets you view or print a list of events that have been stored in the server log.
- The Alarm Monitor lets you view or print a list of alarms generated by the system.

Event Preferences

You might want to customize an event to prevent it from generating an alarm or to limit the number of times it generates an alarm during a specific time interval. You can also customize an event to prevent it from flooding the server log.

- Changing an event's default severity

Events that have a default severity of Critical, Major, or Minor automatically generate alarms. To stop an event from generating an alarm, you can change its default severity from Critical, Major, or Minor to Information. If other users are responsible for monitoring events, notify them before changing the default severity.

- **Throttling an event**

Event throttling lets you control the frequency with which events are recorded by the server log. To throttle an event, specify the interval at which the event is logged and the number of instances that is recorded during that time period.

Event Browser

The Event Browser lets you view events that have been recorded in the server log. You might want to view events if you suspect that there is a problem with system hardware or software, or if system performance has deteriorated. You might also want to view events on a regular basis to ensure that your system is working properly. Use the Event Browser to view the time an event occurred, the object that generated the event, and the cause of the event.

- **Event filtering**

To reduce the number of events shown in the Event Browser at one time, you can set up a filter that screens the log for events that meet your specifications. Events can be filtered according to their code, type, severity, or interval.

- **Filtering and throttling**

Filtering and throttling are easily confused. Filtering is a utility run from the Event Browser that lets you view a list of events that have been stored in the server log. Throttling is controlled from the Event Preferences window and lets you determine how often events are recorded in the server log.

Alarm Monitor

The Alarm Monitor window is used to view the details of alarms. From this window, you can view the details of an alarm, such as the code and severity of the event that raised the alarm, the time at which the event was logged, the program that generated the event, and the cause of the event.

The first time that a Critical, Major, or Minor event triggers an alarm, an entry is created in the Alarm Monitor list. Each time the event occurs, the Alarm Monitor updates the time and date assigned to the alarm. Only one instance of an alarm appears at any time in the Alarm Monitor.

When you have investigated an alarm and decided on an appropriate course of action, you can clear the alarm from the Alarm Monitor.

Disk space usage

Introduction

The performance of your CallPilot system depends, to some degree, on the amount of available disk space. Without enough disk space, the server cannot perform adequately. In some circumstances, the server can stop functioning.

What monitoring disk space involves

For the most part, monitoring disk space involves watching for alarms. You can, however, take a more active role by monitoring

- disk usage
- Nortel directory disk space
- MMFS volumes (which store voice and fax messages and other related multimedia files such as user mailboxes, greetings, voice prompts, and voice menus)
- the database that stores all user information and system statistics, such as the number of calls processed within a certain period of time

Disk usage

The Disk Usage Report in Reporter provides information on the disk usage for all the disk drives on the server.

To conserve server disk space, logfiles older than 90 days are automatically removed at the start of each new backup or restore.

Monitoring the Nortel directory disk space

This involves waiting for alarms to be raised. You can, however, determine how much free space exists on this disk using the Server Performance Monitor (SPM).

Monitoring MMFS volumes

This involves waiting for alarms to be raised as available disk space becomes limited. You can, however, display or print reports on MMFS volume disk usage using Reporter. These reports indicate disk space usage patterns, which can help you plan a strategy to deal with limited disk space.

Monitoring the database

You cannot monitor the database disk space directly. However, an alarm is raised if the database reaches its expected limit.

The database is created during installation and is designed to be large enough to store the full amount of anticipated system data. Under normal operation, the database should never fill up.

In some systems, particularly new ones for which usage patterns have yet to be established, the database might approach its expected limit. If this happens, you must determine the cause and provide a solution.

How disk usage is monitored

The following tools are available for monitoring disk usage:

- **Disk Usage window**
This window is used to view the current status of your hard disk to verify how much disk space is available.
- **Server Performance Monitor**
The SPM provides detailed information on the disk space available on the system.
- **Reporter**
In Reporter, you can view reports about system performance after you perform a download of OM's from the server to your client personal computer.

You can also do the following actions to reduce the amount of used disk space:

- Decrease the amount of time that the system retains messages before they expire if you discover that the MMFS is getting full.

- Reduce the amount of storage space that is allocated to users. You can change this requirement only after the fact (for example, in case a user already has many messages stored in his or her mailbox).
- Reduce the amount of time for which OMs are collected and retained on the hard disk.

Server performance

Introduction

Server performance data provides valuable information about your server's resources. Knowledge of server performance data can help you to

- monitor overall resource usage
- identify periods of abnormal system activity
- predict system resource usage
- determine whether system resources are adequate

How server performance is monitored

Monitor server performance by using the SPM to review information about processor usage, available memory, and available storage space.

You might want to view server performance daily to ensure that the server is working properly. You might also want to view data if your server's performance has deteriorated.

Hardware problems

Detecting hardware problems using fault management

Fault management is a term that describes how the CallPilot server detects and notifies you of potential or real hardware problems (faults).

The following is an overview of how CallPilot monitors hardware problems. For more hardware monitoring and troubleshooting information, see the *Installation and Configuration Guide* for your server type.

Event processing

The CallPilot server processes events to detect hardware problems and raises alarms to notify you when these problems occur.

All events are reported to the Fault Management Server, an invisible subsystem within the server operating system. The Fault Management Server enables the CallPilot server to listen and respond to its clients.

Alarm notification

When an alarm appears in the Alarm Monitor, you must investigate the problem, isolate it, and fix the cause of the problem. This last step clears the alarm from the Alarm Monitor.

Detecting hardware problems

You become aware of a hardware problem when an alarm is raised. All hardware faults produce an alarm (or series of alarms, depending on the problem) in the Alarm Monitor.

Other indications of a hardware-related problem include

- user complaints
- call processing difficulties, such as busy signals, static, dropped calls, trouble connecting, cross talk (hearing other conversations)

- system administrator log on difficulties
- the appearance of an icon on the Maintenance window

Isolating hardware problems

The following elements can be used to isolate hardware problems:

- the Alarm Monitor to investigate one or more raised alarms
- the Event Browser to investigate a series of events that occurred around the time an alarm was raised
- the Maintenance window if you suspect or discover a problem with a particular hardware component

With this window, you can view a component's state to determine whether the component is disabled or off duty.

You can also run diagnostic tests and view their results. Diagnostic test results can help you determine if a piece of hardware needs to be replaced.

You might also want to do the following tasks:

- Check the CallPilot configuration.
If CallPilot is not configured properly, you might get errors such as calls not being answered. If there are complaints about system performance, and you cannot detect a hardware problem, then check the CallPilot configuration.
- Check the switch configuration.
If the switch is not configured properly, it affects the call flow from the switch to the server.
- Check the Service DN table configuration.
If calls are not answered (ringing but no answer), check that the Service DN table is configured properly and that the caller is dialing the correct DN. If a caller is dialing a DN that is not listed in the Service DN table, then the call is not answered.

Introduction

Channels carry digital voice, fax, and speech recognition data from the switch to the server. When the data reaches the server, multimedia channels process the data accordingly, depending on the type of transmission (voice, fax, or speech recognition).

Channel state

If the server has difficulty processing incoming calls, view the state of all channels simultaneously on the client. The following states indicate the current activity or status of each channel. How frequently and when these states change depends on

- which channels are installed and properly configured
- whether a channel is busy transporting data or waiting for a call to be made
- whether a channel has been stopped
- whether a channel is out of service (Off Duty)

How channel states are shown

Each channel is represented by a marker in the Channels window. These markers change color to indicate the current state.

The colors or characters are interpreted by viewing the State Legend and Count at the bottom of the Channels window.

Multimedia channel states

Multimedia channels are configured to process different types of incoming call data; voice, fax, or speech recognition. Each channel is represented by a marker in the Multimedia Channels window. Each marker contains a character that represents the type of media the channel is configured to process.

Stopping and starting channels

Stop channels to take healthy channels out of service before performing diagnostics, upgrades, or installations.

Start channels to put channels back into service following diagnostics, upgrades, or installations. Also, if the problem with an unhealthy channel has been resolved and the channel is ready to be operational, you must start the channel to put it back in service.

Channel distribution

If users are complaining that lines are busy, the distribution of calls over the existing channels might not be balanced. This can occur if the system does not have the optimum distribution of voice, fax, and speech recognition channels. For example, if the system is not receiving many fax calls, there might be some idle fax channels. At the same time, the voice channels might be overloaded. Fax or speech recognition channels can be reassigned to another function to relieve a temporary imbalance in the distribution of calls.

Reports

Introduction

Reporter is a software program that helps you analyze and manage your CallPilot system. Reporter converts raw statistics (Operational Measurements) from your server into easy-to-read reports. These reports can help you to

- establish a baseline pattern of normal system behavior
- monitor system usage
- assess your system's overall efficiency
- detect potential system problems
- monitor system security
- bill users for service usage
- track your administrator-level actions
- plan for future enhancements

Reporter provides reports on the performance of your CallPilot system. You can also configure alerts to warn you when system activity is unsatisfactory or when dangerous performance levels have been reached.

For more information and instructions on how to use Reporter, refer to the *Reporter Guide*.

Establish a baseline

Generate reports on a regular basis to establish a pattern of normal behavior, or "baseline," for your system. A baseline lets you differentiate between normal system activities and unusual or suspicious activities. Once you have established a baseline, you can use reports to identify potential problems.

Evaluate system usage and efficiency

Study reports to help you assess the overall efficiency of your system and decide whether changes are necessary. Among other things, reports can show you

- how long callers wait before their calls are handled
- how many callers abandon their calls
- how often callers access each service or feature
- how many calls are processed by each channel
- how much free disk space is available

Detect potential system problems

Analyze the information in reports to identify potential system problems, such as hardware failures or inadequate resources.

Some of the potential problems that can be detected through reports are

- hardware failures
- inadequate resources
- inefficient usage

Monitor system security

If you are concerned about the security of your system, reports can help you detect potential hacker activity.

Bill service usage

Reports can also help to simplify your billing process. Bill-back reports monitor how often users access services that have a fee associated with them (for example, long distance).

Track administrator actions

Reporter can retrieve and display administrator activities. The Administration Journal provides detailed information about administrator-level actions. It records information on

- user administration, such as changes to users, shared distribution lists, and mailbox classes
- messaging administration, such as changes to message delivery configuration, internet mail clients, security administration properties, and restricted permission lists
- system administration, such as changes to Application Builder

If you need to trace administrator actions, you can create an administration report and customize it using the filtering and sorting options.

Chapter 9

Viewing and filtering server events

In this chapter

About server events	262
Using the Event Browser versus the Alarm Monitor	264
Changing the event log size	266
Using the Windows NT Event Viewer	269
Section A: Using the Event Browser	271
Viewing events in the Event Browser	272
Filtering events in the Event Browser	275
Saving and printing a list of events from the Event Browser	278
Section B: Using the Alarm Monitor	281
Viewing events in the Alarm Monitor	282
Specifying when the Alarm Monitor appears in the foreground	284
Showing the Alarm Monitor in the background	285
Clearing active alarms	286
Section C: Filtering events using the Event Preferences program	289
Throttling events (reducing the frequency of events)	290
Filtering by changing event properties	292
Adding, changing, and deleting event preferences	293
Section D: Configuring CallPilot to send SNMP traps to an NMS	297
Overview	298
Configuring SNMPs on the CallPilot server	299
Configuring an NMS to receive CallPilot traps	302

About server events

Introduction

This chapter describes how to view and filter events that are generated on the server.

Events

Events are occurrences on the CallPilot server, such as applications opening or closing, or errors being reported. Some events are for information only. Events are categorized by severity. These events appear in the CallPilot System window on the administrative PC in the Event Browser and Alarm Monitor, and in the Windows NT Event Viewer on the server. The Alarm Monitor does not report information-level events.

Event severity

Events are assigned a default severity, as described below.

Critical

These events indicate that a service-affecting condition has occurred and an immediate corrective action is required. Critical events are reported when a component is completely out of service and you must take immediate action to restore it. For example, an event can indicate that the file system has crashed.

Major

These events indicate that a service-affecting condition has developed and an urgent corrective action is required. The event condition can cause severe degradation in server performance, and you must restore full capacity. For example, the event can indicate that the file system is 100 percent full.

Minor

These events indicate that a non-service-affecting fault condition exists, and that you must take corrective action to prevent a more serious fault. For example, an event can indicate that the file system is 90 percent full.

Information

These events indicate that something noteworthy has happened on the system, but do not mean that there is a problem. For example, an information-level event can indicate that a service has started or stopped. These events are displayed in the Event Browser but not in the Alarm Monitor.

System events

System events such as Windows NT driver events appear as event code 40592 in the Event Browser and in the system log in the Windows NT Event Viewer.

Security events

Security auditing is enabled on the server. Suspicious actions by a user are logged as event code 40593 in the Event Browser and in the security log in the Windows NT Event Viewer. This is an information event, so it does not appear in the Alarm Monitor.

Using the Event Browser versus the Alarm Monitor

Introduction

The Event Browser and Alarm Monitor both show events that occur on the server. These programs provide many common features for viewing events. The table below lists each feature and the program that offers the feature.

The main advantage for the Event Browser is that you can perform detailed filtering by several categories, including severity and event code range. You can also specify a number of latest events to view, so that you see only recent events.

The main advantage for the Alarm Monitor is that it automatically appears in the foreground of the desktop when an event occurs. This immediately alerts you to a problem. You can specify whether the Alarm Monitor is displayed in the foreground for only critical events, major and critical events, all events, or if it stays in the background.

Event Browser versus Alarm Monitor feature matrix

Feature	in Event Browser	in Alarm Monitor
view events	Yes	Yes
view online Help for an event	Yes	Yes
sort events by category	Yes	Yes
save a list of events	Yes	No
print a list of events	Yes	Yes
view minor, major, critical events	Yes	Yes
view information events	Yes	No

Feature	in Event Browser	in Alarm Monitor
filter events by code, type, severity, latest events	Yes	No
filter events using Event Preferences window	Yes	Yes
automatically show the window in the foreground when an event occurs	No	Yes
clear an event	No	Yes

Changing the event log size

Introduction

The event log resides on the server and stores a record of all events that occur on the server. You must log on to the server to change the event log size.



CAUTION

Risk of affecting server performance

Only qualified Nortel Networks technicians should make changes to the log settings. If you change the size settings, the results affect the performance of the server and the number of events that can be stored.

Event wraparound

The event log size is fixed. It does not increase in size as new events are added to the log. When the log is full and a new event is generated, the server removes the *oldest* event report in the log and replaces that record with the newest one.



CAUTION

Risk of affecting server performance

Do not change the event log wrapping mechanism and size.

Impact of log size changes

If you reduce the size of the event log, then the server can store fewer events. If you increase the event log size, you reduce the amount of available disk space on the server and might slow the response times for retrieving events from the Event Browser.

Application events such as CallPilot events are stored in the Application log. If you change the Application log size, you also change the number of CallPilot events that are stored.

Default event log size

If you change the log size for the CallPilot server, do not use the Default button. The settings for this button correspond to the Windows NT default settings. During a CallPilot installation, the log settings are set to the following defaults:

Log name	Size	Event log wrapping
Application log	8 Mbytes	Overwrite events as needed.
System log	512 kbytes	Overwrite events as needed.
Security log	512 kbytes	Overwrite events as needed.

To change the event log size

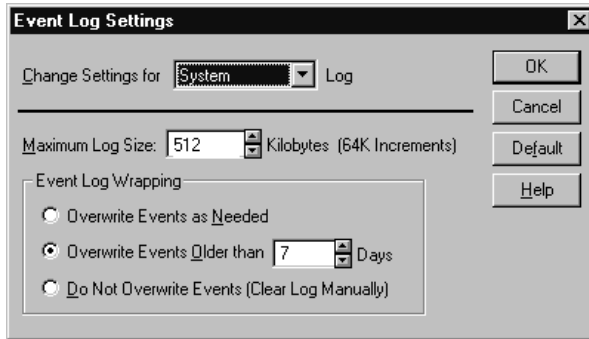
- 1 Log on to the server as Administrator.
- 2 Choose Start > Programs > Administrative Tools (Common) > Event Viewer.

Result: The Event Viewer appears.

Date	Time	Source	Category	Event	User	Computer
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	8:52:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6

- 3 Choose Log > Log Settings.

Result: The Log Settings dialog box appears.



- 4 Change the size of each log in the dialog box.

Note: CallPilot events are stored in the Application log. Change the Application log size to change the number of CallPilot events that are stored.

- 5 Click OK to accept the changes.
- 6 Choose File > Close.

Using the Windows NT Event Viewer

Introduction

The Windows NT Event Viewer on the CallPilot computer provides event and log information. Most information provided by the Event Viewer on the server can also be viewed through the Event Browser on the client on the administrative PC.

When to use

Use the Windows NT Event Viewer on the server to view information that you cannot view through the Event Browser on the client. This information includes

- database events (from the application log)
- server debug events (from the application log)

To open the Windows NT Event Viewer

- 1 Log on to the server as Administrator.
- 2 Choose Start > Programs > Administrative Tools (Common) > Event Viewer.

Result: The Event Viewer appears.

Date	Time	Source	Category	Event	User	Computer
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:16:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	10:04:27 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:52:26 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:40:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:28:25 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:16:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	9:04:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6
12/7/98	8:52:24 AM	BROWSER	None	8011	N/A	ICCMNGEN6

- 3 From the Log menu, select one of the following options:
 - a. Click Application to view application, database, and server debug events.
 - b. Click Security to view security events.
 - c. Click System to view system events.

Section A: Using the Event Browser

In this section

Viewing events in the Event Browser	272
Filtering events in the Event Browser	275
Saving and printing a list of events from the Event Browser	278

Viewing events in the Event Browser

Introduction

The Event Browser shows events that occur on the server.

Default filtering

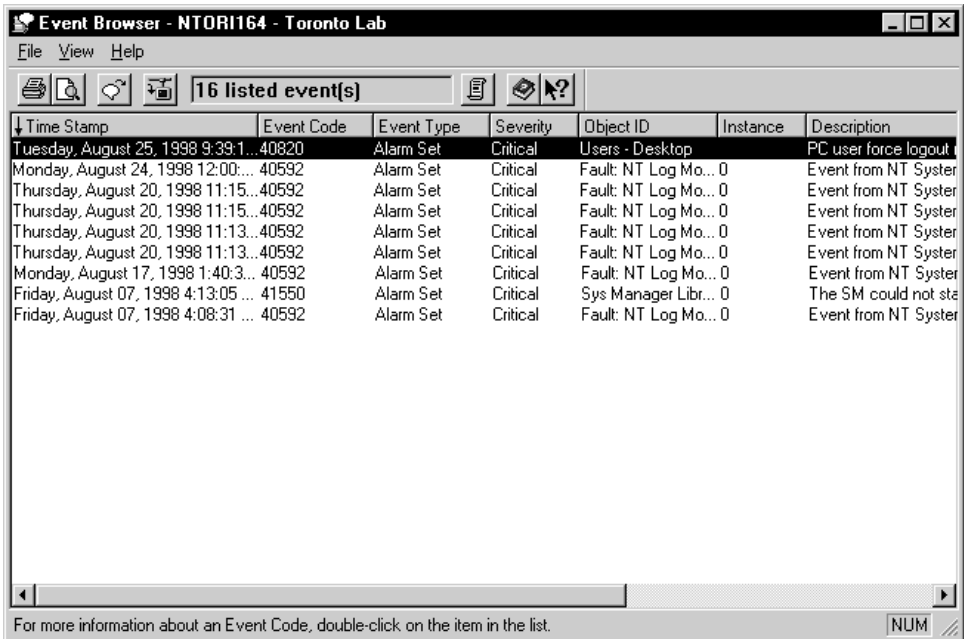
By default, only the latest 100 *critical* events are displayed in the Event Browser. You can change the filter to view all events. For more information, see [“Filtering events in the Event Browser” on page 275](#).

Getting there CallPilot System > System Administration > Alarms & Events > Event Browser

To open the Event Browser

- 1 Select Alarms & Events > Event Browser.

Result: The Event Browser window appears.



- 2 If you must adjust the column widths, place the cursor on the bar between the column heading names and scroll to the left or right.

Sorting events

To sort the list of events in the Event Browser, click the header of the column by which you want to sort. For example, to sort the events by type, click the Event Type header.

Default order

The default order lists the latest event first.

To view help for event codes

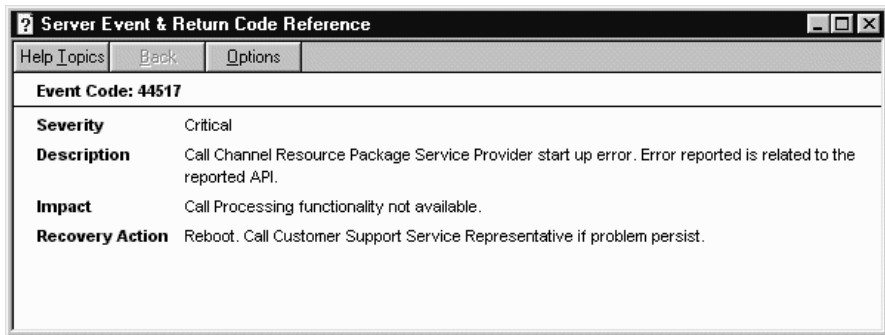
The online Help contains more information about each entry, including a recovery path to correct or further investigate the problem.

- 1 Double-click the event in the Event Browser.

Result: The Event Details dialog box appears.

- 2 Click Help on Event.

Result: Online Help appears for the event. The following is an example.



Filtering events in the Event Browser

Introduction

If you want to reduce the number of events shown in the Event Browser at one time, you can screen the event log to view a specific number of the most recently filtered events.

Filter settings

You can set the filter to display

- a specific number of latest events, or all events that are retrieved from the server
- events of a certain severity (critical, major, minor, information)
- a specific event code range, or all event codes
- a specific type of alarm (alarm set, alarm cleared, or message)
- events that occurred during a specific date and time interval

Note: The filter combines the filter settings from each category.

Default filter

The default filter setting shows the latest 100 critical events.

Example

At BestAir (an imaginary company name used in examples only), system engineer Jane Oliver is testing a new server component. Before she performs the tests, she changes the filtering criteria to display all events, including information events. These events tell her whether system components are starting up or not. When Jane finishes her tests, she changes the filtering criteria back to the default setting.

Getting there

CallPilot System > System Administration > Alarms & Events > Event Browser

To view all events

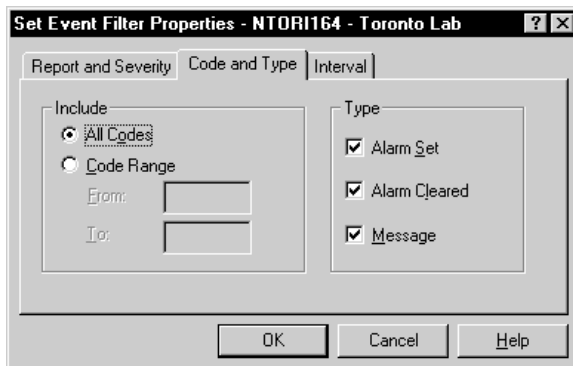
- 1 From the Event Browser, select File > Change filter criteria.

Result: The Set Event Filter Properties window appears. The Report and Severity page appears first.



- 2 Click All Events.
- 3 Click all the Severity levels.
- 4 Click the Code and Type tab.

Result: The Code and Type page appears.

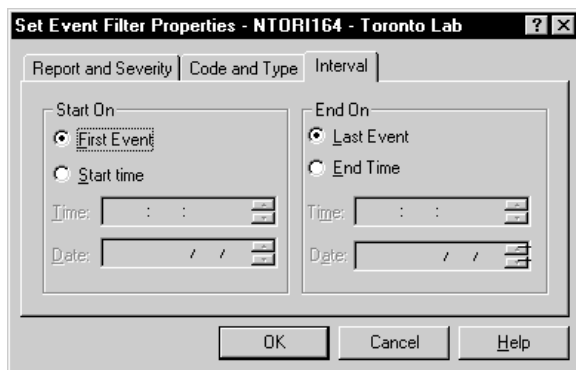


- 5 Click All Codes.

6 Click each box in the Type column.

7 Click the Interval tab.

Result: The Interval page appears.



8 To view all events, ensure that the date and time boxes are blank.

9 Click OK to change the filter.

Result: The Event Browser window is updated and the new and changed event information appears.

To filter events to show a subset of all events

To view a subset of events, follow the steps in “Getting there” on page 276, except specify the criteria (for example, events occurring on a specific day) that you are looking for. Events that match the criteria on all tabs in the Set Event Filter Properties sheet are listed in the Event Browser.

Saving and printing a list of events from the Event Browser

Introduction

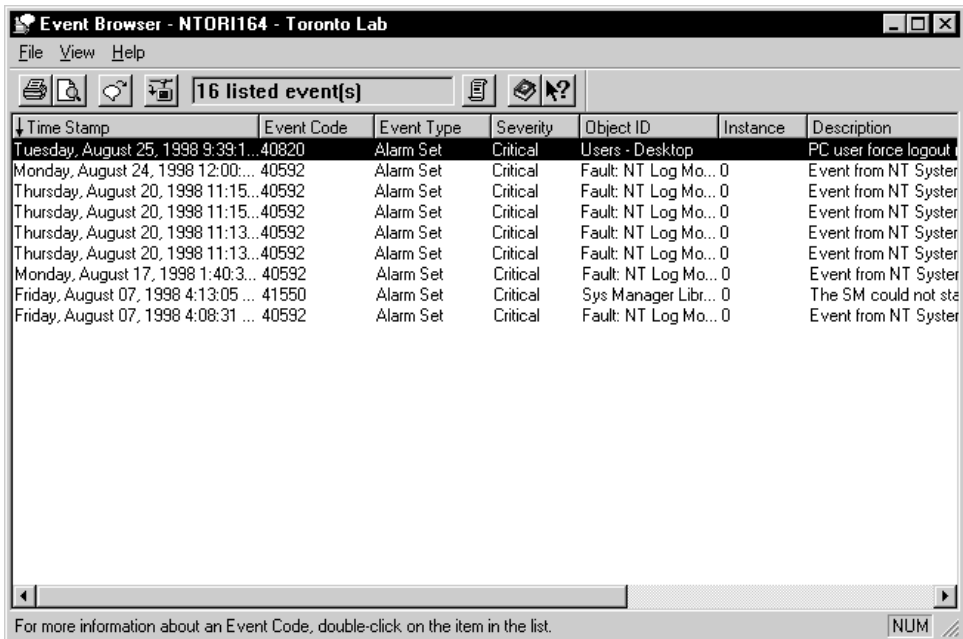
You can save or print any relevant sections of the event log. If you have a problem with your system the log can help technical support representatives conduct a thorough analysis of your system.

Getting there CallPilot System > System Administration > Alarms & Events > Event Browser

To save a list of events into a file

- 1 Select Alarms & Events > Event Browser.

Result: The Event Browser appears.



- 2 If you want to save only some of the events, then highlight the events you want to save.

- 3 Choose File > Save Event Log.

Result: The Save As dialog box appears.

- 4 Select All events (to save a list of all events) or select Selected event(s) to save only the highlighted events.

Note: Ensure that you have selected the specific events you want to save first.

- 5 Click OK.

Result: A dialog box appears for you to provide a filename and select a location.

- 6 Enter a recognizable filename and location.

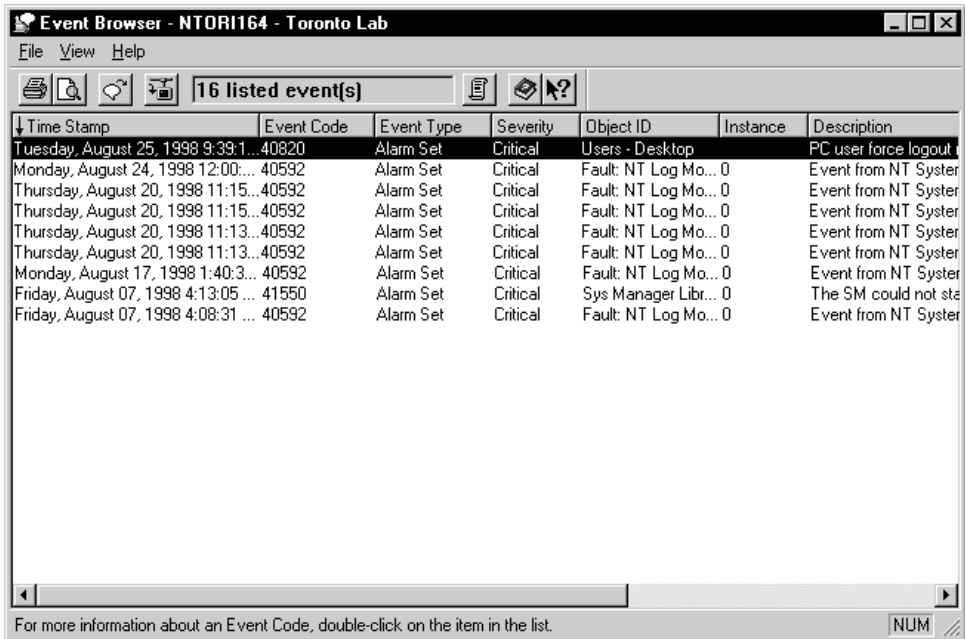
Result: The events are saved in the file you specified.

To print a list of events from the Event Browser

Note: The Print Preview option allows you to preview the print job, and then print your selection.

- 1 From the CallPilot System, select System Administration > Alarms & Events > Event Browser.

Result: The Event Browser appears.



- 2 If you want to print only some events, then press Ctrl and select the events you want to print.
- 3 Choose File > Print.

Result: The Print dialog box appears.

- 4 Click All to print all events or Selection to print only the highlighted events.
- 5 Click OK.

Result: The report prints.

Section B: Using the Alarm Monitor

In this section

Viewing events in the Alarm Monitor	282
Specifying when the Alarm Monitor appears in the foreground	284
Showing the Alarm Monitor in the background	285
Clearing active alarms	286

Viewing events in the Alarm Monitor

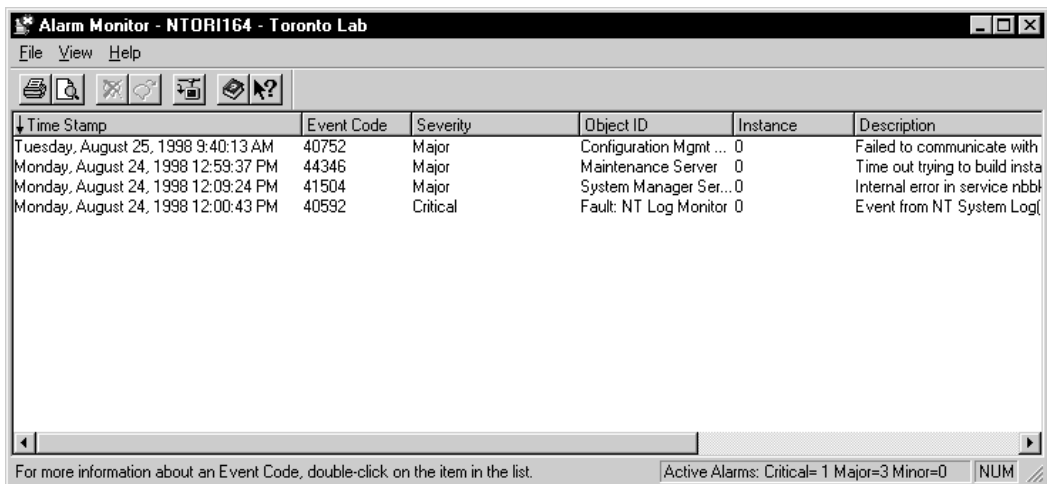
Getting there CallPilot System > System Administration > Alarms & Events > Alarm Monitor

To open the Alarm Monitor

By default, the Alarm Monitor appears in the foreground when an event occurs. If you cannot see the Alarm Monitor or if it has been closed, follow the steps in this procedure.

- 1 Select Alarms & Events > Alarm Monitor.

Result: The Alarm Monitor window appears.



Tip: If you must adjust the column widths, click the cursor on the bar between the column heading names and drag the cursor to the left or right.

To refresh the Alarm Monitor

Choose View > Refresh to update the Alarm Monitor window with current information.

It is possible for the Alarm Monitor to show fewer alarms after refreshing the screen if alarms are cleared by other processes.

Sorting events

To sort the list of events in the Alarm Monitor, click the header of the column by which you want to sort. For example, to sort the events by type, click the Event Type header.

Default order

The default order lists the most recent event first.

To view help for event codes

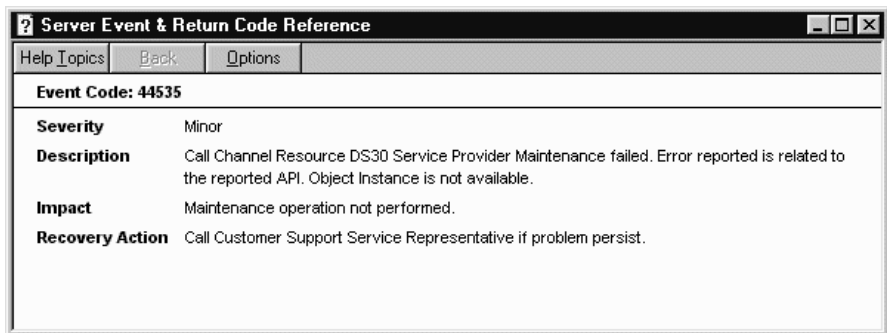
The online Help contains more information about each entry, including a recovery path to correct or further investigate the problem.

- 1 Double-click the event in the Alarm Monitor.

Result: The Event Details dialog box appears.

- 2 Click Help on Event.

Result: Online Help appears for the event. The following is an example.



Specifying when the Alarm Monitor appears in the foreground

Introduction

By default, the Alarm Monitor appears in the foreground of your display when any event occurs. However, you can specify the severity of alarm that determines when the Alarm Monitor appears in the foreground.

To specify when the Alarm Monitor appears in the foreground

From the CallPilot Administration Client, select the Utilities menu. Click one of the following options:

- Alert All Alarms - This option shows the Alarm Monitor window every time an alarm is registered or updated.
- Alert Major and Critical Only - This option shows the Alarm Monitor window every time a Major or Critical alarm is registered or updated.
- Alert Critical Only - This option shows the Alarm Monitor window every time a Critical alarm is registered or updated.

Showing the Alarm Monitor in the background

When to use

If you do not want to see the Alarm Monitor every time it receives and updates a new alarm, you can set it to appear in the background of your display.

To set the Alarm Monitor to appear in the background

From the CallPilot Administration Client, select the Utilities menu. Click Alerting Off.

Result: The Alarm Monitor is moved to the background. When a critical alarm is registered, the Alarm Monitor window taskbar flashes until the Alarm Monitor window is brought to the foreground.

Note: If you select Alerting Off and then minimize the Alarm Monitor, the minimized Alarm Monitor flashes when a critical alarm is registered until the Alarm Monitor window is restored.

Clearing active alarms

When to use

You can clear alarms from the Alarm Monitor in one of two ways:

- The CallPilot server automatically clears alarms when the alarm condition changes.
- You can clear alarms manually.

When you clear an alarm you remove the selected alarm (but not the event that raised it) from the active alarm list. You also remove the selected alarm from the list shown in the Alarm Monitor. If the event occurs again, however, the alarm reappears in the Alarm Monitor.

Example

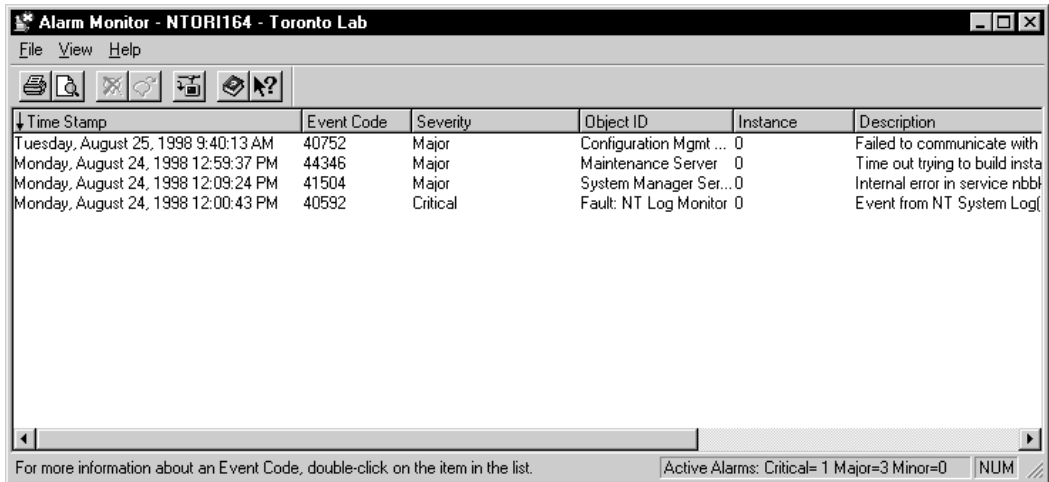
At BestAir, an alarm appears with the description “Disk is 90% full.” Mark Brown, the system administrator, checks the system disk space, removes temporary files, and considers ordering a larger hard drive. Only after he has resolved the problem does he clear the alarm from the Alarm Monitor.

Getting there CallPilot System > System Administration > Alarms & Events > Alarm Monitor

To clear an alarm

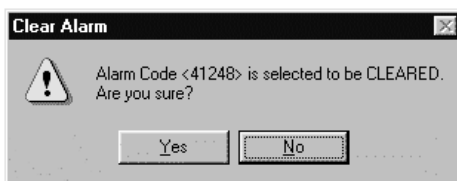
- 1 Select Alarms & Events > Alarm Monitor.

Result: The Alarm Monitor window opens.



- 2 Select the alarm you want to clear.
- 3 Choose File > Clear Alarm.

Result: A dialog box asks you to confirm that you would like to clear the selected alarm.



- 4 Click Yes.

Result: The alarm entry is removed from the Alarm Monitor.

Section C: Filtering events using the Event Preferences program

In this section

Throttling events (reducing the frequency of events)	290
Filtering by changing event properties	292
Adding, changing, and deleting event preferences	293

Throttling events (reducing the frequency of events)

Introduction

Event throttling lets you control the frequency with which the same event is recorded by the event log and appears in the Event Browser, Alarm Monitor, and Windows NT Event Viewer. This prevents these windows and the event log from becoming overcrowded. If too many instances of each event are recorded, there might not be enough space in the event log to record more important events. Also, viewing too many instances of each event can overwhelm users, causing them to overlook important events.

To set throttling on only specific event codes

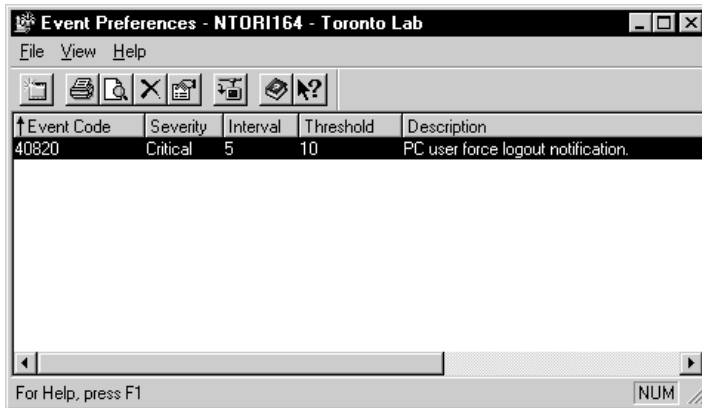
To set throttling on specific event codes, see [“Adding, changing, and deleting event preferences” on page 293](#).

Getting there CallPilot System > System Administration > Alarms & Events > Event Preferences

To define throttling parameters for all events

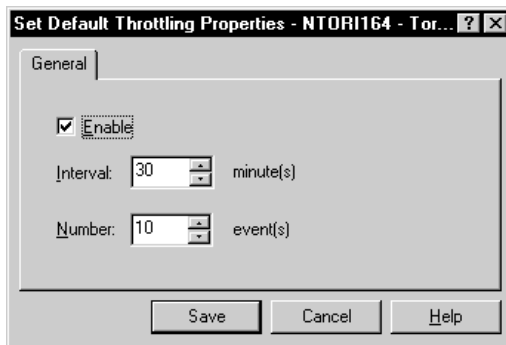
- 1 Select Alarms & Events > Event Preferences.

Result: The Event Preferences window appears.



- 2 Choose File > Default Throttling.

Result: The Set Default Throttling Properties window appears.



- 3 Select Enable.
- 4 Type a value in the Interval and Number boxes. This determines the number of times the same event (Number box) can be recorded in the Event Log in a period of time (Interval box).
- 5 Click Save to apply the throttling properties and to return to the Event Preferences window.

Filtering by changing event properties

Introduction

You might want to override the default severity or throttling parameters of any event code for the following reasons:

- to increase the severity of an event (for example, from information to minor) so that the event is displayed in the Alarm Monitor when it occurs
- to reduce the severity of a recurring alarm to information so that the event does not appear in the Alarm Monitor
- to set the throttling parameters to reduce the frequency an event is generated

Previous occurrences of the event are not affected. You can revert to the default event definition at any time by deleting the event preference for that event code.

Adding an event preference to change the properties of an event

The Event Preferences program enables you to add an event preference for an event code. In the event preference, you can specify the severity and throttling parameters for a specific event code. See [“Adding, changing, and deleting event preferences” on page 293](#).

Example

At BestAir, CallPilot server is generating a critical alarm because of a database error. The system engineer, Jane Oliver, has ordered a replacement for the malfunctioning disk drive that is causing the problem. Since she is aware of the problem, Jane does not want to see an alarm on her console every time the error occurs.

Jane can add an event preference for this event code to reduce the severity of the error from critical to information. After the new disk is installed, she can delete the event preference to restore the severity to critical.

Adding, changing, and deleting event preferences

Introduction

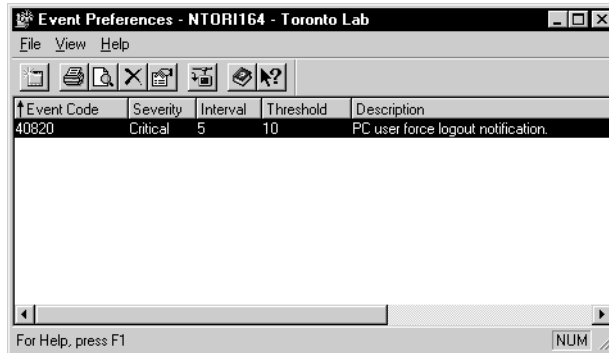
When you add an event preference, you can change the default severity or throttling parameters for a specific event code. For examples and more explanation, see [“Filtering by changing event properties” on page 292](#).

Getting there CallPilot System > System Administration > Alarms & Events > Event Preferences

To add an event preference

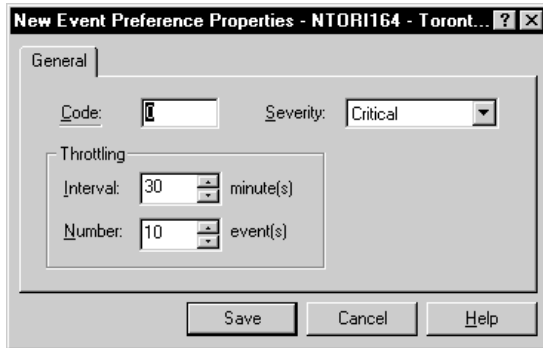
- 1 From System Administration, select Alarms & Events > Event Preferences.

Result: The Event Preferences window appears.



- 2 Choose File > New.

Result: The New Event Preferences Properties sheet appears.



- 3 In the Code box, type the event code for which you want to change the default severity or throttling parameters.

Note: The CallPilot server does not accept unrecognized event codes. For a complete list of valid event codes, go to the Event Browser and select Event Code Reference from the Help menu.

- 4 From the Severity drop-down list box, select the severity you want to assign to the event.
- 5 Fill in the Interval and Number boxes. These boxes enable you to limit the number of times (Number box) the event can be recorded in the Event Log in a period of time (Interval box).

Example: In 30 minutes (the interval), allow the event to be logged a maximum of 10 times (the number).

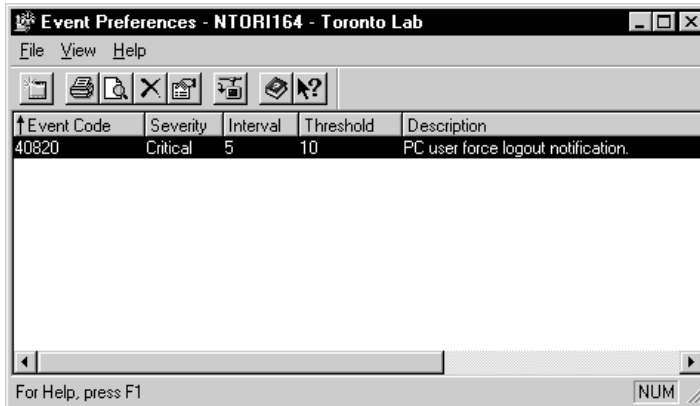
- 6 Click Save to apply the event preference.

Result: The event preference is added to the Event Preferences window.

To change an event preference

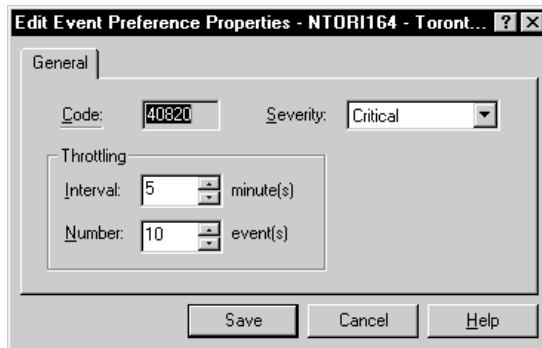
- 1 From the CallPilot System, select System Administration > Alarms & Events > Event Preferences.

Result: The Event Preferences window appears.



- 2 Double-click the event preference you want to change.

Result: The Edit Event Preference Properties sheet appears.

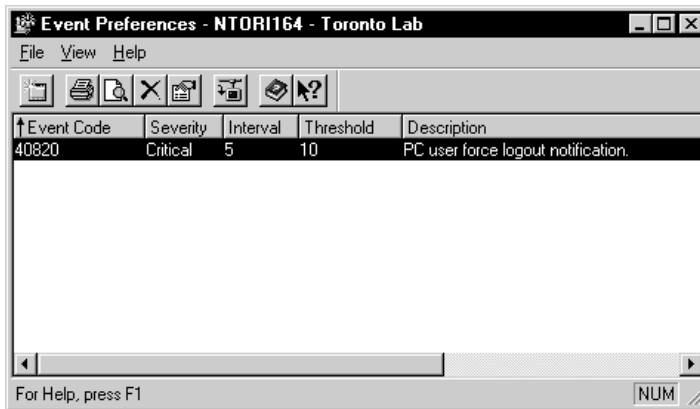


- 3 Modify the settings as required.
- 4 Click Save apply the changes.

To delete an event preference

- 1 From the CallPilot System, select System Administration > Alarms & Events > Event Preferences.

Result: The Event Preferences window appears.



- 2 Select the event preference you want to delete.

Result: The event preference is highlighted.

- 3 Choose File > Delete.

Result: A dialog box appears asking you to confirm that you want to delete the entry.

- 4 Click Yes to confirm the deletion.

Result: The entry is deleted from the window.

- 5 To return to the CallPilot Administration Client, choose File > Exit.

Section D: Configuring CallPilot to send SNMP traps to an NMS

In this section

Overview	298
Configuring SNMPs on the CallPilot server	299
Configuring an NMS to receive CallPilot traps	302

Overview

Introduction

This section describes how to configure the CallPilot server to send Simple Network Management Protocols (SNMP) traps to a Network Management System (NMS). When this service is configured you can work with server alarms on an NMS.

Two examples of NMS clients that you can configure to use this service are the MAT Alarm Notification and the HP Openview tools. The procedure in this section uses the MAT Alarm Notification tool as one example of how to configure an NMS.

The configuration has two parts:

- configuring SNMP on the CallPilot server so that the traps are directed to an NMS
- configuring the NMS so that it can receive the CallPilot SNMP traps

Configuring SNMPs on the CallPilot server

Introduction

Windows NT provides a Simple Network Management Protocol (SNMP) v1 agent that runs as a service on the CallPilot server. This service can be configured so that the SNMP traps generated by the CallPilot server are directed to a Network Management System (NMS) that resides on your site network.

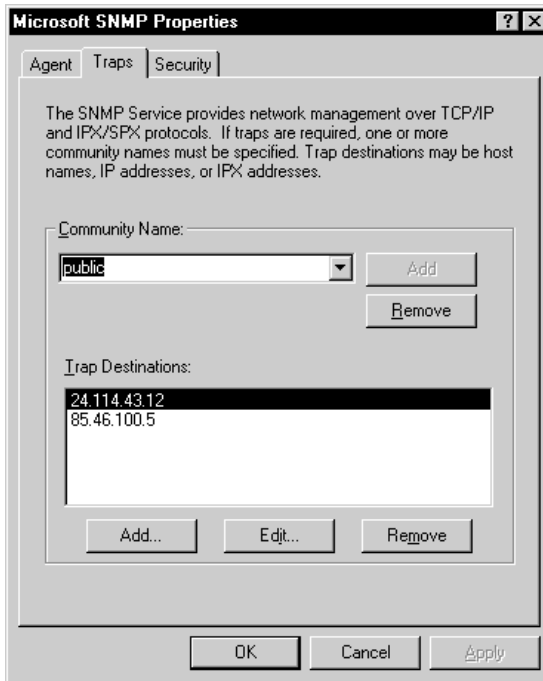
In the following procedure, you stop the SNMP service, configure SNMP, and then restart the SNMP service.

To configure SNMP to forward traps to an NMS

- 1 On the CallPilot server, select Start > Settings > Control Panel. Double-click Services.
Result: The Services window appears.
- 2 In the Services list, select SNMP.
- 3 Click Stop.
Result: The SNMP service stops.
- 4 Click Close.
Result: The Services window closes.
- 5 From the Control Panel, double-click Network.
Result: The Network window appears.
- 6 Select the Services tab.

- 7 In the list of Network Services, select SNMP Service. Click Properties.

Result: The Microsoft SNMP Properties window appears.



- 8 Select the Traps tab.
- 9 If no community name is defined in the Community Name field, type **public**. Click Add.
- 10 To add a trap IP destination, go to the bottom of the Trap Destinations list box and click Add.
- Result:** The Service Configuration window appears.
- 11 Type in the trap IP address of the NMS you want to use. Click Add.
- Result:** The IP address is added.
- 12 Repeat steps [10](#) and [11](#) to add all the NMS clients that you want to receive the traps.
- 13 Click OK.

Result: The Microsoft SNMP Properties window closes.

14 Click Close.

Result: The Network window closes.

15 From the Control Panel, double-click Services.

Result: The Services window appears.

16 In the Services list, select SNMP.

17 Click Start.

Result: The SNMP service starts.

18 Click Close.

Result: The Services window closes.

Configuring an NMS to receive CallPilot traps

Introduction

Once the CallPilot server is configured to send traps to an NMS, then you configure the Network Management System (NMS) to receive these traps.

The following procedure uses the MAT Alarm Notification tool as an example of how to configure an NMS.

Network Management Systems

There are a number of NMS systems that you can use to receive and interpret traps. Each one requires a different setup.

This chapter covers the MAT Alarm Notification NMS only. However, by using the CallPilot Management Information Base (MIB) files it should be possible to set up other NMS systems to interpret CallPilot traps.

Management Information Base files

The CallPilot SNMP MIB files describe the CallPilot trap format. The network administrator might want to look at these files when configuring an NMS to receive CallPilot SNMP traps.

The MIB files are nbflt.mib and nt-ref.mib. They are SNMP v1 MIB files and can be used on an NMS system.

The MIB files are available

- on the CallPilot Server CD, in the directory platform\default\nortel\data\
- on the CallPilot server in the directory D:\Nortel\data\

Alarms

The CallPilot server generates alarms. Alarms with the following severity levels are sent out as SNMP traps to the NMS:

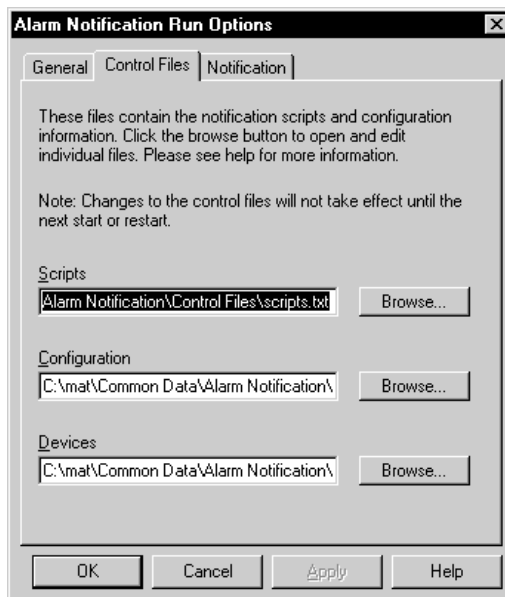
- 0 undefined
- 1 critical
- 2 major
- 3 minor

To configure MAT Alarm Notification to receive CallPilot SNMP traps

- 1 From the MAT Alarm Notification window, select Configuration > Run Options.

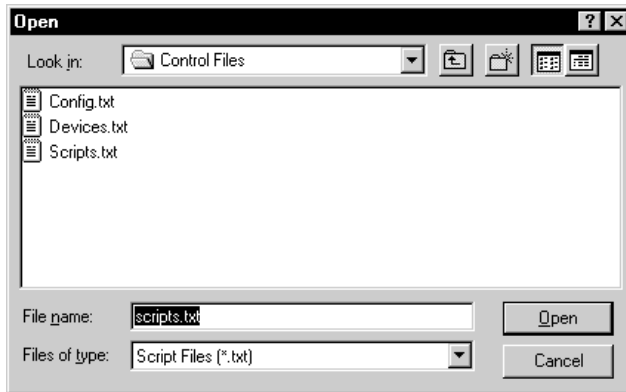
Result: The Alarm Notification Run Options Property Sheet appears.

- 2 Select the Control Files tab. The Control Files tab lists three files: Devices.txt, Config.txt, and Scripts.txt. You must modify each of these files.



- 3 To modify Devices.txt, click Browse beside the file name.

Result: The Open dialog box appears with the file name selected.



- 4 Click Open.

Result: The file opens in an editor where you can modify the file.

- 5 Modify the file as follows:

■ FILE: Devices.txt

In this file, add the following line:

```
CALL_PILOT IP_ADDRESS_OF_SERVER
```

where:

CALL_PILOT is the name displayed under Device Type in the MAT Alarm Notification window. It can be any value.

IP_ADDRESS_OF_SERVER is the actual IP address of the server that sends the traps to this NMS client.

Example: CALL_PILOT 47.235.12.85

- 6 To modify Config.txt, click Browse beside the file name.

Result: The Open dialog box appears with the file name selected.

- 7 Click Open and Modify the file as follows:

■ FILE: Config.txt

In this file, add the following block of text:

...


```

device CALL_PILOT 6.1 6.2 6.3 6.4 {
    1.3.6.1.4.1.562.3.8.1.5.2.1.2.0 string
    $nbFltAlarmTimeStamp "Event Time"

    1.3.6.1.4.1.562.3.8.1.5.2.1.3.0 integer
    $nbFltAlarmEventCode "Error Code"

    1.3.6.1.4.1.562.3.8.1.5.2.1.4.0 integer
    $nbFltAlarmEventType "Alarm Type"

    1.3.6.1.4.1.562.3.8.1.5.2.1.5.0 integer
    $nbFltAlarmEventSeverity "Severity"

    1.3.6.1.4.1.562.3.8.1.5.2.1.8.0 string
    $nbFltAlarmOriginator "Component Name"

    1.3.6.1.4.1.562.3.8.1.5.2.1.9.0 string
    $nbFltAlarmDescription "Operator Data"
}

```

...

where:

CALL_PILOT is the same name that is defined in the Devices.txt file.

- 8 To modify Scripts.txt, click Browse beside the file name.

Result: The Open dialog box appears with the file name selected.

- 9 Click Open and modify the file as follows:

- FILE: Scripts.txt

In this file, add the following blocks of text:

...

```

/* This is a sample definition for using a log file. All events sent to this
notification are appended to the filename defined below. Note that Windows
"long" file names are not supported. */

```

```

notification file CALLPILOT_file {
    filename:="c:\Nortel\callpilot_log.txt";
}

```

...

```

/* This is a sample definition for using a numeric pager */

```

```

notification npager CALLPILOT_NumericPager {
    phone:="9,378-6388";
    ...
    /* if pager has PIN number insert */
    /* pin:="101565"; */
}
...
where:
CALLPILOT_NumericPager is any name (it is used in the script code
below)
"9,378-6388" is the pager number
...

/*****/
/* Scripts for CALLPILOT Traps */
/*****/
/* Add the following lines */
script CALLPILOTScript {
    /* This rule looks for all CallPilot events and remaps them to the
    MAT event format */
    rule check_critical {
        if ($CurrentTrapDevice="CALL_PILOT") {
            /* Prints event to MAT Alarm Notification console - optional*/
            send(con,"CALLPILOT alarm: ",
$nbFltAlarmTimeStamp," - " ,
$nbFltAlarmEventCode," - " ,
$nbFltAlarmEventType," - " ,
$nbFltAlarmEventSeverity," - ",
$nbFltAlarmOriginator," - ",

```

```
$nbFltAlarmDescription);  
    /* Appends event to log file - optional*/  
    send(CALLPILOT_file,"NGEN alarm: ",  
$nbFltAlarmTimeStamp," - " ,  
$nbFltAlarmEventCode," - " ,  
$nbFltAlarmEventType," - " ,  
$nbFltAlarmEventSeverity," - ",  
$nbFltAlarmOriginator," - ",  
$nbFltAlarmDescription);  
    /* Sends message to numeric pager - optional */  
send(NGEN_NumericPager,$nbFltAlarmEventCode);  
  
    }  
}  
}  
...
```

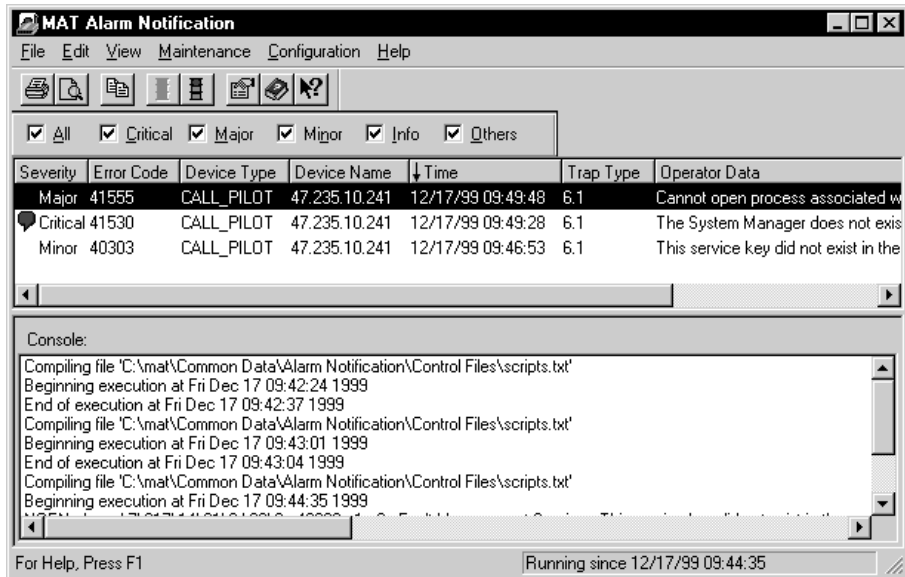
Note: These three files are located in [MAT]\Common Data\Alarm Notification\Control Files where [MAT] is usually C:\MAT.

10 After modifying the files, click OK.

Result: The Alarm Notification Run Options Property Sheet closes.

- 11 In the MAT Alarm Notification window, select Maintenance > Start.

Result: CallPilot traps appear in the MAT Alarm Notification window list view as they are generated by the CallPilot server.



Chapter 10

Viewing and filtering client PC events

In this chapter

Overview	310
Viewing client PC events	311
Filtering events in the PC Events browser	312

Overview

Introduction

This chapter describes how to view and filter events that are generated on the client PC.

Viewing client PC events

Default filtering

By default, all client PC events are shown in the PC Events browser. You can change the filter to view all events. For more information, see [“Filtering events in the PC Events browser” on page 312](#).

Getting there CallPilot Administration Client Explorer > Utilities > PC Events

To open the PC Events browser

- 1 Double-click PC Events.
Result: The PC Events browser window opens.
- 2 If you need to adjust the column widths, place the cursor on the bar between the column heading names and scroll to the left or right.

Sorting events

To sort the list of events in the PC Events browser, click the header of the column by which you want to sort. For example, to sort the events by User, click the User header.

Refreshing the window

The window is automatically updated every five seconds. To update the window immediately with the latest events, click View > Refresh.

Filtering events in the PC Events browser

Introduction

Filtering is a process that enables you to select the types of events you want to view. Filter events if you do not want to see all events, or if you want to see only specific types of events.

When you open the PC Events browser, all events are shown regardless of any filter you have defined. Before you can view only filtered events, you must create the filter using the Change Filter Criteria option, and then apply the filter.

You can filter events according to severity, code, user ID, site, and system. The filter criteria that you define for each category are combined to create one filter. If you are not satisfied with the filter, you can make changes or clear filter settings.

Getting there CallPilot Administration Client Explorer > Utilities > PC Events

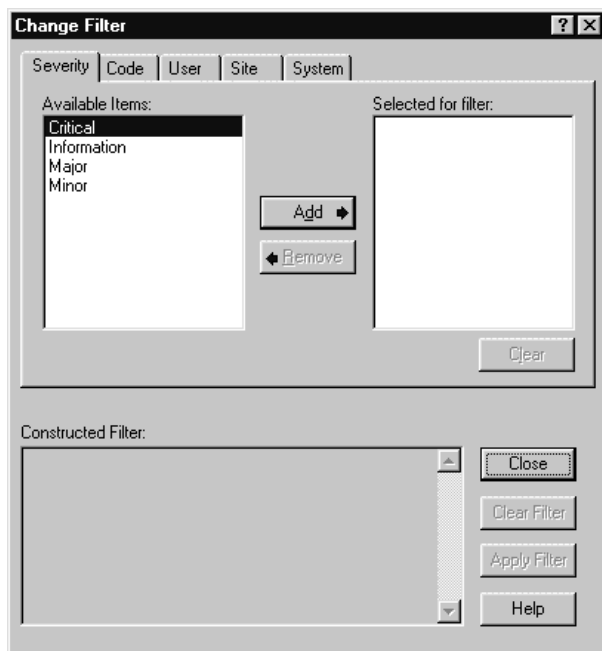
To create a filter or to change the filter criteria

ATTENTION

The filter does not take effect until you click Apply Filter in the Change Filter Criteria window. You have to apply the filter each time you open the PC Events browser in order for the filter to take effect. The filter does not automatically stay in effect.

- 1 In the PC Events browser window, on the File menu, click Change Filter Criteria.

Result: The Change Filter property sheet appears. This property sheet includes tabs for the different categories of possible filter criteria: Severity, Code, User, Site, System.



- 2 Click the Severity tab.
- 3 Click the criteria in the Available Items list that you want to include and then click Add to include them in the Selected for filter list.

- 4 Repeat steps [2](#) and [3](#) for each tab that contains criteria you want to include in the filter.

Result: The combined filter that includes all the filter criteria from each tab is shown in the Constructed Filter field.

Note: You can use the Clear button to clear filter criteria from the current tab. You can use the Clear Filter button to clear filter criteria from all tabs.

- 5 If you want to apply the filter, click Apply Filter.
- 6 When you are satisfied with the filter, click Close to save and exit.

Chapter 11

Monitoring the server

In this chapter

Section A: Viewing switch configuration and server settings	317
About switch configuration and server settings	318
Viewing the switch settings	319
Viewing the server settings	320
Section B: Monitoring disk space	323
Overview	324
Monitoring Nortel directory disk space	326
Monitoring Multimedia File System volumes	327
General methods to monitor disk space	330
Section C: Monitoring the database	333
Monitoring the database using alarms	334
Section D: Monitoring server performance	337
About the Server Performance Monitor	338
Viewing server performance data	339
Printing server performance data	341

Section A: Viewing switch configuration and server settings

In this section

<u>About switch configuration and server settings</u>	<u>318</u>
<u>Viewing the switch settings</u>	<u>319</u>
<u>Viewing the server settings</u>	<u>320</u>

About switch configuration and server settings

Introduction

This section describes how to view information about the current switch settings and CallPilot server settings on your system. You might need this information when you communicate with product support personnel.

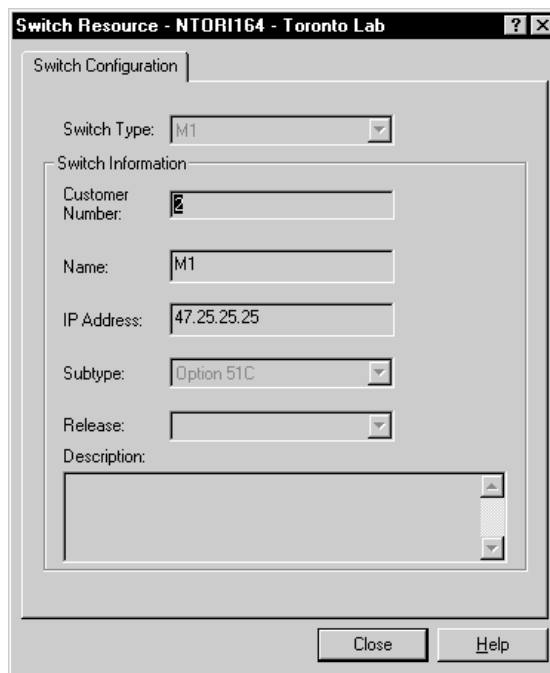
Switch configuration is performed during the installation of the CallPilot application. You cannot reconfigure the switch from the client. For more information on configuring the switch, see the *Installation and Configuration Guide* specific to your server.

Viewing the switch settings

Introduction

Use the Switch Resource window to view the current switch settings.

Getting there CallPilot System > System Administration > System Configuration > Switch Resource



The screenshot shows a window titled "Switch Resource - NTORI164 - Toronto Lab". Inside, there is a "Switch Configuration" tab. The "Switch Type" is set to "M1". Below this is a "Switch Information" section containing several fields: "Customer Number" (2), "Name" (M1), "IP Address" (47.25.25.25), "Subtype" (Option 51C), "Release" (empty), and "Description" (empty text area). At the bottom of the window are "Close" and "Help" buttons.

Field	Value
Switch Type	M1
Customer Number	2
Name	M1
IP Address	47.25.25.25
Subtype	Option 51C
Release	
Description	

Viewing the server settings

Introduction

The Server Settings window on the administrative PC shows information about your CallPilot system, including the following elements:

- system name
- software version (release) number
- serial number
- keycode
- feature information

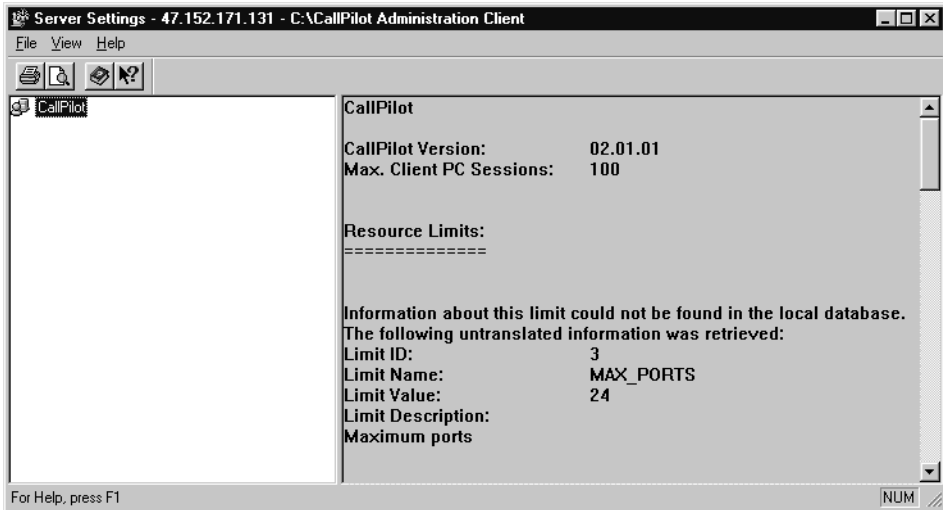
Getting there CallPilot System > System Administration > System Configuration > Server Settings

To view server settings

- 1 From System Administration, select System Configuration > Server Settings.

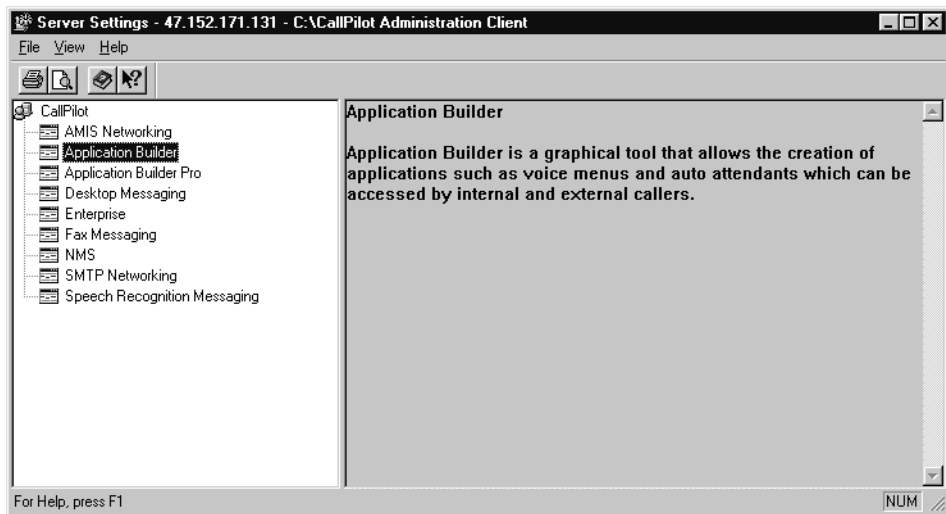
Result: The Server Settings window appears.

Note: Based on the type of switch that you have and the features included in your keycode, the content of your window might vary from the example below.



- 2 In the left pane, click on CallPilot to see information about the CallPilot server system.

- 3 In the left pane, click on a feature to see information about that feature.



- 4 Choose File > Close to exit from the Server Settings window.

Section B: Monitoring disk space

In this section

Overview	324
Monitoring Nortel directory disk space	326
Monitoring Multimedia File System volumes	327
General methods to monitor disk space	330

Overview

Introduction

This section describes the general steps to take to maintain an even distribution of data on your system hard disk so that it performs efficiently and to capacity.

The performance of your CallPilot system depends, to some degree, on the amount of available disk space. Without enough disk space, the server cannot perform adequately. In some circumstances, the server can stop functioning.

Nortel Networks systems are engineered to provide adequate space to meet your data storage and system operation requirements. You must, however, monitor disk space occasionally to ensure space does not become too limited.

Disk partitions

Disk partitions refers to two partitions of the disk:

- The Multimedia File System (MMFS) contains messages and greetings and other changing CallPilot data.
- The database includes administrative information such as user profiles, which include user names and directory numbers, and operational measurements (OMs), which are raw data about the system.

What monitoring disk space involves

For the most part, monitoring disk space involves watching for alarms. You can, however, take a more active role by monitoring the following units of storage:

Nortel directory disk space

You can determine the percentage of free disk space for the fixed disk containing the Nortel directory using the Server Performance Monitor (SPM).

For more information on monitoring the Nortel directory disk space, see [“Monitoring Nortel directory disk space” on page 326](#).

MMFS volumes

The MMFS volumes store all voice and fax messages and other related multimedia files, such as user mailboxes, greetings, voice prompts, and voice menus.

Of all the disk space on the system, the MMFS volumes are most likely to fill up first. Monitor them frequently to determine any changes in usage patterns.

For more information on monitoring MMFS volumes, see [“Monitoring Multimedia File System volumes” on page 327](#).

The database

The database stores all user information and system statistics, such as the number of calls processed within a certain time period.

For more information on monitoring the database, see [“Monitoring the database” on page 333](#).

Nightly audit deletes expired files

Each night, the CallPilot server performs an audit that cleans up expired files in the Multimedia File System and the system database.

In particular, the audit removes user messages from the MMFS that have passed their expiry date and expired OMs from the system database.

See also

For more information on the hard disk and the MMFS, see the *Installation and Configuration Guide* for your server type.

Monitoring Nortel directory disk space

Introduction

To monitor the disk space available for the Nortel directory, you must wait for alarms to be raised. You can, however, determine how much free space exists on this disk using the Server Performance Monitor (SPM).

For information on how to use the Server Performance Monitor, see [Section D: “Monitoring server performance,” on page 337](#).

Alarms

Although you can use the SPM to monitor the Nortel directory disk space, alarms are raised if logical disk space becomes limited. Different alarms are raised depending on how much disk space is left on the logical drives.

Alarm	Amount of space left
Major	less than 10%
Critical	less than 5%

Monitoring Multimedia File System volumes

Introduction

The MMFS volumes store all voice and fax messages and other related multimedia files, such as user mailboxes, greetings, voice prompts, and voice menus. The server can have more than one volume, depending on the overall capacity of the system to process calls. When an MMFS volume is full, no new files can be created on that volume.

If an MMFS volume has less than 10 percent of disk space left, you must free up enough space to clear the alarms.

Note: When you lower the retention period for user messages you do not affect the database. You must be clear about which parts of the hard disk (either the database or the MMFS) are approaching a point where they are nearly full.

What monitoring MMFS volumes involves

Monitoring MMFS volumes involves waiting for alarms to be raised as available disk space becomes limited. You can, however, display or print reports on MMFS volume disk usage using Reporter. These reports indicate disk space usage patterns, which can help you to plan a strategy to deal with limited disk space.

Alarms

Although you can use Reporter to monitor MMFS volumes, alarms are raised as MMFS volumes fill up. Different alarms are raised, depending on how much disk space is left for the MMFS volume.

Alarm	Amount of space left
Major	less than 10%
Critical	less than 5%

When alarms are raised, a warning box appears indicating the volume ID and the percentage full. To clear an alarm, you must free up disk space on the MMFS volume for which the alarm was raised.

Clearing alarms

Alarms are cleared when less than 88 percent of MMFS volume disk space is being used. To clear alarms, you must free up space on the MMFS volume for which the alarm was raised.

- If one MMFS volume is full while other volumes are empty, you can move users' mailboxes from the full volume to another one.
- Disk space usage patterns on voice mail systems fluctuate, because voice messages are constantly created and deleted. If all volumes are filling up, you can do the following actions to reduce the size of mailboxes:
 - Send a broadcast message asking users to delete unneeded messages.
 - Look at user usage reports to determine which users are using a lot of space, and talk to them about it.
 - Delete unneeded mailboxes that might be filling up with broadcast messages.
 - Reduce the maximum space allowed for some or all mailboxes so the system tells users their mailboxes are full.
 - Reduce the read message retention time on some or all mailboxes so that the automatic message deletion cleans up more messages sooner.
- In an application using automatic read message deletion, disk usage typically increases from Monday to Friday. Disk usage decreases over the weekend as read messages are deleted and few new ones are created. When

you understand these patterns you can better plan a strategy to deal with disk space problems.

- If the system is chronically low on space, consider purchasing additional storage from Nortel Networks, particularly if you need to add new users to the system.

General methods to monitor disk space

Introduction

You have several ways to monitor how much disk space is available on your system.

Disk Usage window

In the Disk Usage window, available from the System window, you can view the current status of your hard disk to verify how much disk space is available.

Server Performance Monitor

The Server Performance Monitor (SPM) provides detailed information on the disk space available on the system.

Refer to [Section D: “Monitoring server performance.” on page 337.](#)

Reporter

In Reporter, you can view reports about system performance after you perform a download of OMs from the server to your administrative PC.

The Multimedia File System Usage report helps you determine if the level of user messages is getting too high. The Disk Usage Report provides information on the usage of all disk drives on the server.

For more information, refer to the *Reporter Guide*.

Administrative actions

You can perform certain actions to reduce the amount of used disk space.

Message retention

Decrease the amount of time that the system retains messages before they expire if you discover that the MMFS is getting full.

Storage space

Reduce the amount of storage space that is allocated to users. You can change this requirement only after the fact (for example, in case a user already has many messages stored in his or her mailbox).

OM retention

The system database collects OMs on the hard disk depending on the type of specified OMs and for a specified amount of time. If the database is getting full, reduce the amount of time for which those OMs are collected and retained on the hard disk.

ATTENTION

Because the hard disk is partitioned, reducing the message retention time affects only the MMFS. Reducing the OM retention time affects only the database storage levels.

See also

For more information on message retention and storage space allocation, refer to “Setting up mailbox classes” in the *Administrator’s Guide*.

For more information on OM retention, refer to [Chapter 2, “Configuring operational measurements.”](#)

Section C: Monitoring the database

In this section

[Monitoring the database using alarms](#)

[334](#)

Monitoring the database using alarms

Introduction

The database stores user information, system configuration information, and various statistics that are collected by the system. You cannot monitor the database disk space directly. However, an alarm is raised if the database reaches its expected limit.

Database limits

The database is created during installation. It is designed to be large enough to store the full amount of anticipated system data. Under normal operation, the database should never fill up.

In some systems, particularly new ones for which usage patterns have yet to be established, the database can approach its expected limit. If this happens, you must determine the cause and provide a solution.

ATTENTION

As a precaution against disk failure, the database expands slightly to accommodate data beyond the anticipated limit. However, this is a safety feature. The underlying problem must be addressed as soon as possible.

Causes and solutions

System and user information use only small amounts of database disk space and will not fill up the database. The following are likely reasons why the database reaches its anticipated limit:

OMs are too detailed or stored for too long

OMs are statistics collected by the system. Based on the level of detail and the length of time for which these statistics are stored in the database, more or less disk space is used.

To reduce the amount of OM data that is collected, you must reduce the retention period or change the level of detail for which the system collects statistics. See [Chapter 2, “Configuring operational measurements”](#)

Note: When you lower the retention period for OMs you do not affect the MMFS. Similarly, lowering the retention period for user messages has no impact on the database. You must be clear about which parts of the hard disk (either the database or the MMFS) are approaching a point where they are nearly full.

The system is under-engineered

Systems are shipped with a database large enough to accommodate the initial requirements of customers. If your estimated usage patterns change or if your number of users grow, you might need to purchase additional disk space. Contact your distributor for details.

Section D: Monitoring server performance

In this section

About the Server Performance Monitor	338
Viewing server performance data	339
Printing server performance data	341

About the Server Performance Monitor

Introduction

This chapter describes how you can monitor the day-to-day hardware and software operations of your system.

The Server Performance Monitor (SPM) lets you keep track of the day-to-day hardware and software operations of your system. The window includes information about processor usage, available memory, and available storage space. You might want to view server performance daily to ensure that the server is working properly. You might also want to view data if your server's performance has deteriorated.

Server performance data

Server performance data provides valuable information about your server's resources. This data lets you

- monitor overall resource usage
- identify periods of abnormal system activity
- predict system resource usage
- determine whether system resources are adequate

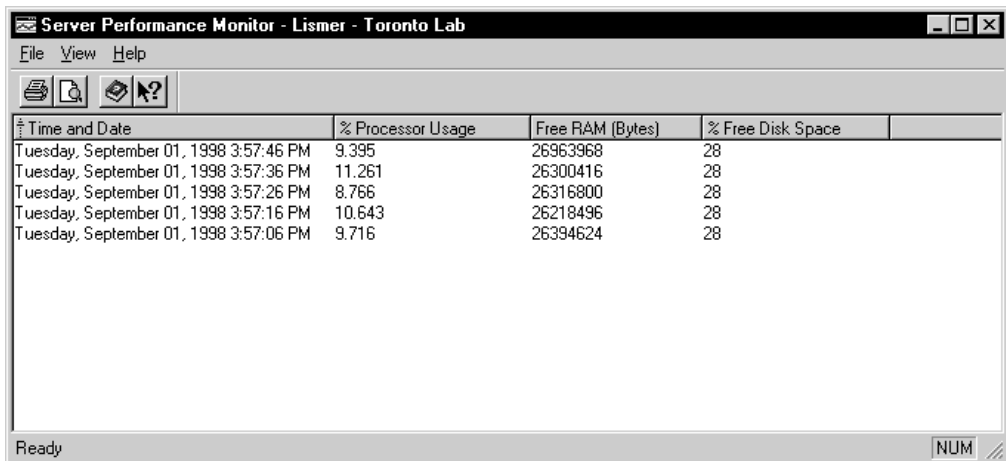
Note: Server performance data is updated every ten seconds.

Viewing server performance data

Introduction

You can view server performance data daily to ensure that the server is working properly. You can also view data if your server's performance has deteriorated.

Getting there CallPilot System > System Administration > System Performance Monitoring > Server Performance Monitor



The screenshot shows a window titled "Server Performance Monitor - Lismar - Toronto Lab". It has a menu bar with "File", "View", and "Help". Below the menu bar is a toolbar with icons for printing, finding, and help. The main area contains a table with the following data:

Time and Date	% Processor Usage	Free RAM (Bytes)	% Free Disk Space
Tuesday, September 01, 1998 3:57:46 PM	9.395	26963968	28
Tuesday, September 01, 1998 3:57:36 PM	11.261	26300416	28
Tuesday, September 01, 1998 3:57:26 PM	8.766	26316800	28
Tuesday, September 01, 1998 3:57:16 PM	10.643	26218496	28
Tuesday, September 01, 1998 3:57:06 PM	9.716	26394624	28

The status bar at the bottom shows "Ready" and a "NUM" button.

The Server Performance Monitor window

The SPM window displays a list of server performance data. Each row represents a snapshot of the state of the server at a particular point in time. Details of each event are displayed in columns under appropriate headings.

When to contact technical support

When using the SPM, consider contacting technical support in the following situations:

If CPU usage (% Processor Usage) remains near 100 percent

If CPU usage occasionally peaks to 100 percent, but generally remains below 80 percent, there is no need for concern. If CPU usage consistently peaks at 100 percent, system limits might have been reached. You might need to upgrade to a platform with a higher CPU capacity.

ATTENTION

High CPU usage can result in lost calls and a slow system response time.

If free disk space is consistently below 15 percent

If free disk space is consistently below 15 percent, you might require more disk space. You might also need to clean up the current disk or database.

If memory usage is consistently near 100 percent

If memory usage is consistently near 100 percent, you might require more memory. High memory usage can also indicate that system processes are consuming memory without releasing it when they are finished.

ATTENTION

High memory usage causes frequent disk swapping and severely degrades system performance.

Printing server performance data

Introduction

You might want to print system performance data if system performance has started to deteriorate and you want to track its progress.

Getting there CallPilot System > System Administration > System Performance Monitoring > Server Performance Monitor

To print selected data

- 1 Click the server performance data that you want to print.

- 2 On the File menu, click Print.

Result: The Print dialog box appears.

- 3 Click Selection for the Print Range.

- 4 Click OK.

Result: A copy of your report prints on your default printer.

To print all data

- 1 On the File Menu, click Print.

Result: The Print dialog box appears.

- 2 Click All for the Print Range.

- 3 Click OK.

Result: A copy of your report prints on your default printer.

Chapter 12

Managing channels

In this chapter

Section A: Managing call channels	345
Overview	346
About call channels and their states	347
Viewing call channel states	352
Starting and stopping call channels	355
Section B: Managing multimedia channels	359
Overview	360
About multimedia channels	361
Viewing multimedia channel states	367
Viewing multimedia channel media types	370
Powering multimedia channels on and off	371
Starting and stopping multimedia channels	373

Section A: Managing call channels

In this section

Overview	346
About call channels and their states	347
Viewing call channel states	352
Starting and stopping call channels	355

Overview

Introduction

Call channels carry digital voice, fax, and speech recognition data from the switch to the server. When the data reaches the server, the multimedia channels process the data according to the type of transmission.

You can monitor individual call channels through the Channel Monitor window to ensure that the distribution of calls is as balanced as possible, and to view the state of all channels. As required, call channels can also be removed from service to perform diagnostics, upgrades, or installations. When the maintenance or diagnostics are complete, the call channels are restarted and put back into service, as outlined in [“Starting and stopping call channels” on page 355](#).

ATTENTION

In this release of CallPilot, there are limitations on starting and stopping call channels on Rolm, Lucent and Mitel switches.

See “Stopping call channels” on page 357 for complete information and procedures.

About call channels and their states

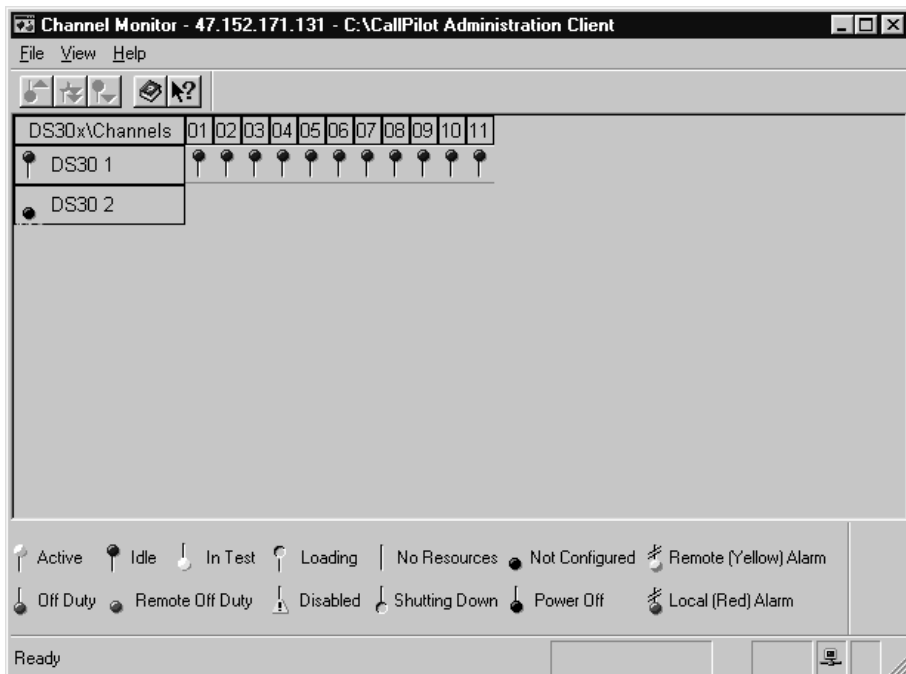
Introduction

Call channels run on links between the switch and server to carry digital voice data. The state of each call channel configured on the system is monitored through the Channel Monitor window.

By default, the Channel Monitor window refreshes every five seconds to display any changes in the state of a call channel. You can change the refresh rate to one or two seconds. For detailed instructions, see [“To change the refresh rate” on page 354](#).

Channel Monitor window

The Channel Monitor window displays the state of all call channels configured on the system.



The Channel legend that appears near the bottom of the window interprets the channel indicator icons to indicate whether a channel is active, idle, off duty, and so on. For an explanation of the call channel states, refer to [“Channel states” on page 349](#).

The status bar at the bottom of the Channel Monitor window displays status information for a selected channel, including

- the configured location of a selected call channel and its state (for example, (1,4) Idle) where:
 - 1** is the number of the card
 - 4** is the number of the selected channel
 - Idle** is the current state of the selected channel
- the icon showing the operational status of the switch
- the directory number (DN) for the selected call channel (for example, 3236104)
- the icon showing the operational status of the server
- the icon showing the operational status of the Simplified Message Desk Interface (SMDI) link



Note: If an icon is marked with an X, the associated switch or server is not operational.

Call channel coordinates

You can identify a call channel's physical location by viewing its location in the Channel Monitor window. Click any call channel and its coordinates are displayed in the status bar at the bottom of the Channel Monitor window. For example, if you select the first call channel on the second card, the status bar displays the coordinates (2,1) for the second card, first call channel (Card 2, Port 1).

The coordinates and status of each call channel can also be identified by holding the cursor over the selected call channel. The coordinates for the call channel and its current state are displayed. For example, call channel 3 on link #2 might appear as

(2,3) Idle

Channel states

The channel state, or current activity, for each call channel on the system is displayed on the Channel Monitor window. The reason and frequency that these states change depends on whether the channels are

- installed and properly configured
- busy transporting data or waiting for incoming data
- stopped or out of service (Off Duty)

A legend explaining the meaning of the color and position for each channel marker is displayed at the bottom of the Channel Monitor window. The following table lists the available channel states, and provides a brief description of the meaning of each state.

Channel state	Description
Active	The call channel is working and currently transporting call data from the switch to the server.
Idle	The call channel is working but not currently transporting call data from the switch to the server.
In Test	The call channel is undergoing diagnostic testing.
Loading	The call channel has been started, which takes it out of the Off Duty state. This state occurs quickly and is immediately followed by the Idle state.
No Resources	The hardware required for call channels to operate is not installed or not operating properly.

Channel state	Description
Not Configured	The hardware has been installed, but the call channel has not been properly configured.
Remote (Yellow) Alarm	A yellow alarm is sent by the receiving T-1 device to the transmitter device. It indicates to the transmitter device that a red alarm condition exists at the receiver device. The yellow alarm is sent for as long as the red alarm condition exists at the receiver device.
Off Duty	<p>The call channel has been stopped.</p> <p>The channel might have stopped as the result of a problem with the channel, a problem with a parent component, or someone taking the channel off duty.</p>
Remote Off Duty	The call channel was taken out of service at the switch.
Disabled	The call channel has been disabled, perhaps as the result of a failed diagnostic or hardware failure.
Shutting Down	The call channel has been stopped. This state occurs quickly and is immediately followed by the Off Duty state.
Power Off	The electrical current has been turned off to the selected card.
Local (Red) Alarm	A red alarm condition occurs when Receive Loss of Synchronization (RLOS) has existed for 2.5 seconds (default) on incoming data. This condition exists until the synchronization has been recovered and remains recovered for 12 seconds (default).

Disabled channels

A call channel can be put into a Disabled state as a result of a failed diagnostic test or hardware failure on the call channel card.

If a call channel fails a diagnostic test, it is put into a Disabled state. The call channel must pass the same diagnostic test before it is put into the Off Duty state. Once the channel is in Off Duty state you can return it to the Idle state. Refer to the diagnostic test results for instructions on how to fix the call channel. You can view the diagnostic test results through the Diagnostic pane of the Maintenance program.

If a call channel is placed in a Disabled state as the result of a hardware problem, the hardware problem must be corrected before the call channel is put back into the Off Duty state. Once the channel is in Off Duty state you can return it to the Idle state. Run diagnostic tests on the call channel from the Maintenance program to determine the cause of the problem. After the problem is corrected, rerun diagnostics to ensure that the call channel is operational.

Once the problem has been corrected, the channel must be restarted, as outlined in [“To start off-duty channels” on page 356](#).

Viewing call channel states

Introduction

Use the Channel Monitor window to view the state of all call channels simultaneously in the Channel Monitor window on the client to determine whether channels are Active, Idle, Off Duty, or Disabled.

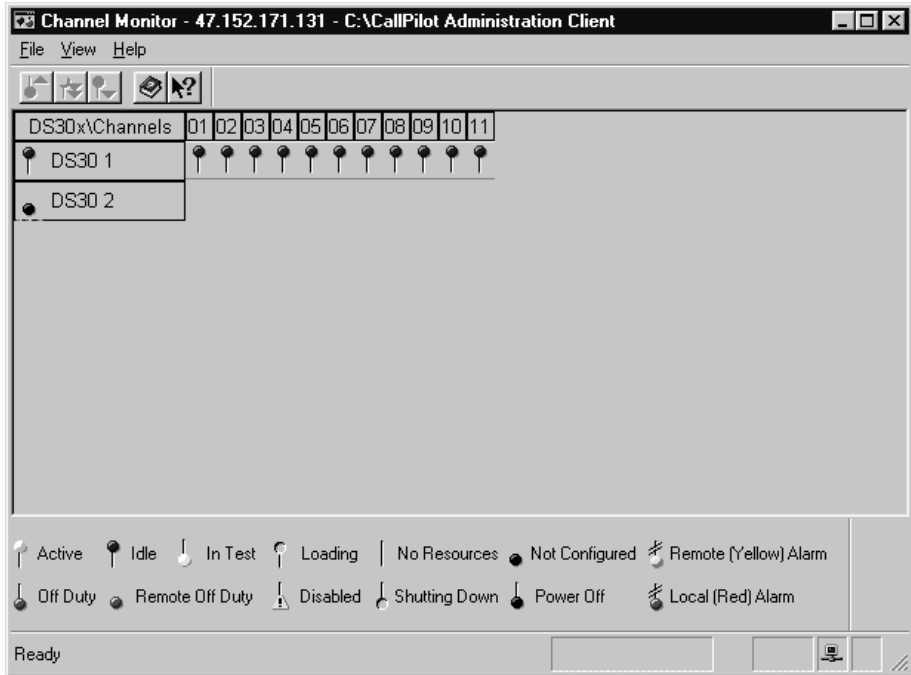
If channels are Off Duty, Remote (Yellow) Alarm, or Local (Red) Alarm, use the Hardware maintenance utility to diagnose the problem.

Getting there CallPilot System > System Administration > Maintenance Administration > Channel Monitor

To view call channel states

- 1 Double-click Channel Monitor.

Result: The Channel Monitor window appears, showing the state of all call channels on the system. For an explanation of the channel states, refer to [“Channel states” on page 349](#).



Refresh rate

By default, the Channel Monitor window refreshes every five seconds. Any changes in the state of a call channel display when the window updates.

You can change the rate at which the Channel Monitor window refreshes to one second or two seconds if you require more frequent updates.

Note: Increasing the refresh rate increases the load on the server because this increases the traffic between the server and the client.

To change the refresh rate

- 1 In the Channel Monitor window, click View > Refresh Rate.
- 2 Select one of the following:
 - 1 sec.
 - 2 sec.
 - 5 sec.

Starting and stopping call channels

Introduction

The following procedures are performed from the Channel Monitor.

Getting there CallPilot System > System Administration > Maintenance
Administration > Channel Monitor

Starting call channels

Introduction

After diagnostics, upgrades, or installations have been completed, or problems with an unhealthy channel have been resolved, you must start the channel to put it back into service.

When a channel is started, the state of the channel is changed from Off Duty to Idle to wait for data to transport from the switch to the server.

You can start an individual call channel, more than one call channel, or all call channels in the Channel Monitor window. Only Off Duty channels can be started.

Note: You can also start individual call channels from the Maintenance tab of the Maintenance window.

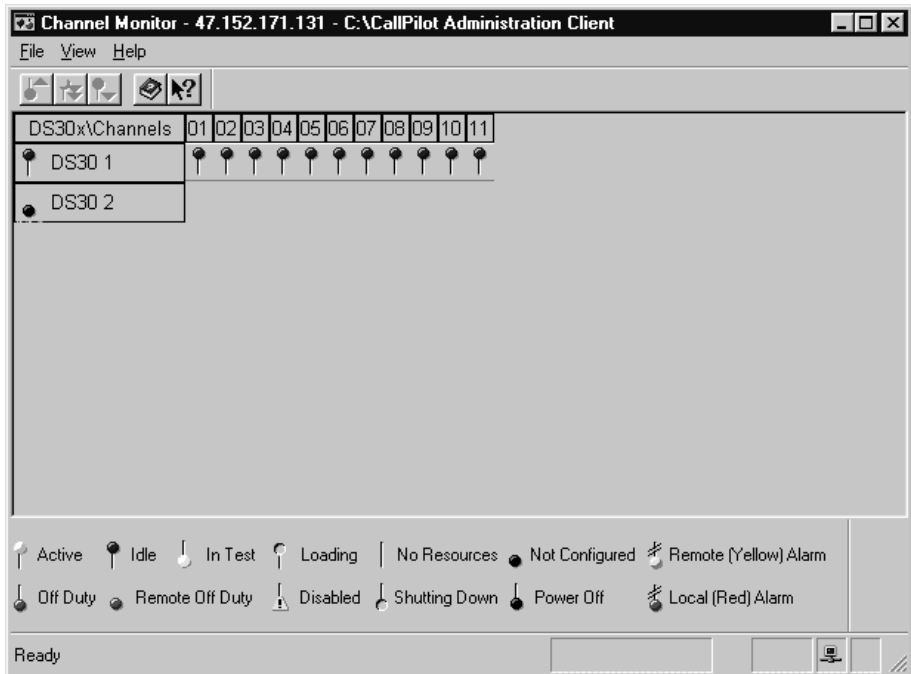
When to start channels

Start call channels after the system has been powered up following an upgrade or installation, or after a diagnostic has been completed.

If a call channel is Off Duty for any other reason (such as Disabled status), you must isolate the cause of the problem and take appropriate action to fix it. For example, you can run diagnostics on the call channel from the Maintenance tab of the Maintenance program to check if there is a problem with the call channel. Off Duty channels start up as soon as they are operational.

To start off-duty channels

- 1 From the Channel Monitor window, select the individual channel or range of channels that you wish to start, as follows:
 - To select all call channels in the system, click the Channels type heading on the top left corner of the call channels columns.
 - To select all call channels for a particular card, click the card button in the left column.
 - To select a specific number call channel, click the call channel number heading (for example, 04).
- 2 Select File > Start, or click Start on the toolbar to start the selected channels.



- 3 Wait a few seconds for the channel state to be updated.
- 4 Verify that the selected call channels have changed status to Idle (or Active).

Stopping call channels

Introduction

Call channels are stopped to take healthy channels out of service before performing diagnostics, upgrades, or installations, or if there is a problem with a channel or the system. When a channel is stopped, it is placed on Off Duty status. While in this state, the call channel cannot carry any voice, fax, or speech recognition data from the switch to the server.

You can stop an individual call channel, more than one call channel, or all call channels in the Channel Monitor window. Only active or idle call channels can be stopped.

CAUTION

For CallPilot servers connected to a Lucent, Mitel, or Rolm switch, if you stop an individual call channel, the corresponding port on the switch side is not automatically disabled. As a result, calls can continue to land on the stopped channel resulting in a Ring-No-Answer (RNA).

If you need to stop an individual channel, you have two options:

- Busy-out the port on the switch side. This must be done manually by the switch administrator.
- Courtesy stop the entire hunt group that contains the call channel or courtesy stop all call channels in the system.

This caution does not apply to stopping DSP ports.

Once the problem with an unhealthy channel has been resolved and the channel is ready to be operational, you must start the channel to put it back in service, as outlined in [“To start off-duty channels” on page 356](#).

Note: You can also start and stop individual call channels from the Maintenance tab of the Maintenance window.

Methods of stopping

There are two methods that can be used to stop a channel: stop or courtesy stop.

- Stop

A stop puts an active or idle call channel into Off Duty state immediately, even if it is busy transporting call data. All calls using these channels are disconnected. Use a stop only when severe problems occur that are affecting a large number of calls or if your organization determines a special need for it.

- **Courtesy stop**

A courtesy stop waits until the channel has finished transporting call data before putting it into Off Duty status. No calls using these channels are interrupted.

When to stop channels

Typically, you courtesy stop call channels before performing diagnostics, upgrades, or installations.

To stop channels

- 1 From the Channel Monitor window, select the individual channel or range of channels that you wish to stop, as follows:
 - To select all call channels in the system, click the Channels type heading on the top left corner of the call channels columns.
 - To select all call channels for a particular card, click the card name in the left column.
 - To select a specific number call channel, click the call channel number heading (for example, 04).
- 2 Determine whether you want to perform a courtesy stop or stop. Refer to [“Methods of stopping” on page 357](#) for an explanation of the difference.
- 3 Select File > Courtesy Stop or File > Stop, or click Courtesy Stop or Stop on the toolbar to stop the selected channels.
- 4 Wait a few seconds for the channel state to be updated.
- 5 Verify that the selected call channels have changed status to Off Duty.

Section B: Managing multimedia channels

In this section

Overview	360
About multimedia channels	361
Viewing multimedia channel states	367
Viewing multimedia channel media types	370
Powering multimedia channels on and off	371
Starting and stopping multimedia channels	373

Overview

Introduction

Call channels carry digital voice, fax and speech-recognition data from the switch to the server. When the data reaches the server, the multimedia channels process the data according to the type of transmission.

You can monitor individual multimedia channels or entire MPC-8 cards through the Multimedia Monitor window to ensure that the distribution of calls is as balanced as possible, and to view the state of all channels. As required, channels can also be removed from service to perform diagnostics, upgrades, or installations. When the maintenance or diagnostics are complete, the multimedia channels are restarted and put back into service, as outlined in [“Powering multimedia channels on and off” on page 371](#).

This chapter fully describes the procedures required to monitor, stop, and start multimedia channels. Instructions to power the multimedia channels on and off are also included.

About multimedia channels

Introduction

As voice, fax, and speech recognition data reaches the server from the switch, the timeswitch on the MPB-16 board routes the data to multimedia channels. Up to 96 multimedia channels provide processing services to the incoming call data, depending on the system.

The state of each multimedia channel and the associated MPC-8 card configured on the system is monitored through the Multimedia Monitor window.

By default, the Multimedia Monitor window is refreshed every five seconds to display any changes in the state of a channel. The refresh rate can be modified to one or two seconds, if required. Refer to [“To change the refresh rate” on page 354](#) for detailed instructions.

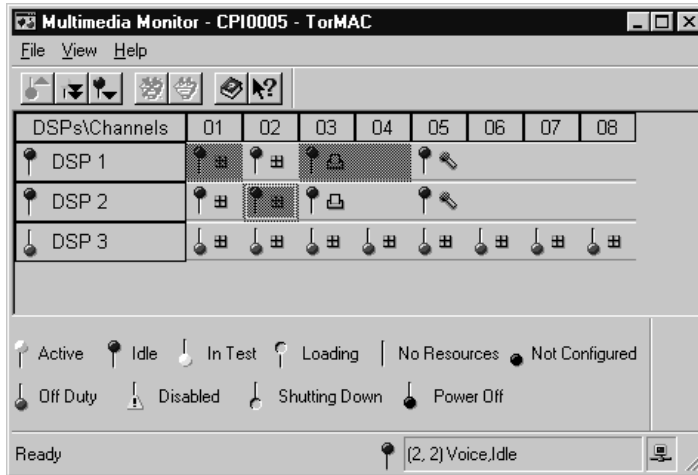
Number of available multimedia channels

Multimedia channels are provided in two forms. Two MPC-8 cards are embedded on an MPB-16 board, and up to four additional removable MPC-8 cards can be inserted into slots on the MPB-16 board.

Each MPC-8 card (embedded or removable) supports up to eight multimedia channels. A fully loaded MPB-16 board contains two embedded MPC-8 cards (2 X 8 channels = 16 channels) and four removable MPC-8 cards (4 X 8 channels = 32 channels) for a total of 48 channels per board. A maximum of two MPB-16 boards can be loaded on the system, which provides a maximum of 96 channels per system.

Multimedia Monitor window

The Multimedia Monitor window displays the state of all multimedia channels configured on the system.



The Channel legend that appears near the bottom of the window interprets the channel indicator icons to indicate whether a channel is active, idle, off duty, and so on. For an explanation, refer to [“Channel states” on page 364](#).

The status bar at the bottom of the Multimedia Monitor window displays status information for a selected channel, including

- the configured location of a selected multimedia channel and its state (for example, **(2,2) Voice, Idle**, where
 - 2** is the number of the MPC-8 card
 - 2** is the number of the selected channel
 - Voice** is the configured allocation for this channel
 - Idle** is the current state of the selected channel)
- the icon showing the operational status of the server




Note: If the icon is marked with an X, the associated server is not operational.

Media types

Multimedia channels are configured to process different types of incoming call data: voice, fax, or speech recognition.

The number of multimedia channels required to process an incoming call depends on the type of data that is being processed. Voice requires one channel, fax requires two channels, and speech recognition requires four channels to process the incoming data. To best use the resources of the system, these channels can be reconfigured as required, based on time of day, day of the week, or other parameters.

Each multimedia channel is represented by a special icon in the Multimedia Monitor window. Each icon represents the type of media the channel is configured to process, as illustrated on the following table:

Icon	Channel media type	Number of Channels required
	Voice	1
	Fax	2
	Speech recognition	4

By monitoring the type and activity of multimedia channels, you can determine whether channels are configured as voice, fax, or speech recognition. This information can help you to determine if you need to reconfigure the channels or add MPC-8 cards to increase the multimedia processing capacity of the server.

Multimedia channel coordinates

You can identify a multimedia channel's physical location by viewing its location in the Multimedia Monitor window.

Click any multimedia channel to display the coordinates, media type, and status of the selected channel in the status bar at the bottom of the Multimedia Monitor window. For example, if you select the first multimedia channel on the second card, the status bar displays the coordinates (2,1) for the second card, first multimedia channel (Card 2, Port 1).

The coordinates and status of each multimedia channel can also be identified by holding the cursor over the selected multimedia channel. The coordinates for the multimedia channel and its current state are displayed. For example, fax channel 3 on link #2 might appear as

(2,3) Fax, Idle

Channel states

The channel state, or current activity, for each multimedia channel and MPC-8 card on the system is displayed on the Multimedia Monitor window. The reason and frequency that these states change depends on whether the channels or cards are

- installed and properly configured
- busy transporting data or waiting for incoming data
- stopped or out of service (Off Duty)

A legend explaining each channel icon is displayed at the bottom of the Multimedia Monitor window. The following table lists the available states and provides a brief description of each one.

State	Description
Active	<p>The multimedia channel is working and currently processing call data, or has completed call processing in the last 30 seconds.</p> <p>The channel remains active for 30 seconds after completing processing in anticipation of receiving future calls.</p>
Idle	The multimedia channel is working and available but not currently processing call data.
In Test	The channel is undergoing diagnostic testing.
Loading	The channel has been started, which takes it out of the Off Duty state. This state occurs quickly and is immediately followed by the Idle state.
No Resources	The hardware required for the multimedia channel to operate is not installed or not operating properly.
Not Configured	The hardware has been installed, but the channel has not been properly configured.
Off Duty	<p>The multimedia channel has been stopped.</p> <p>The channel might have stopped as the result of a problem with the channel, a problem with a parent component, or someone taking the channel off duty.</p>
Disabled	The multimedia channel has been disabled, perhaps as the result of a failed diagnostic or hardware failure.
Shutting Down	The multimedia channel has been stopped. This state occurs quickly and is immediately followed by Off Duty.
Power Off	The electrical current has been turned off to the selected card.

Disabled channels

A multimedia channel or card can be put into a Disabled state as a result of a failed diagnostic test or hardware failure on the multimedia channel card.

If a channel fails a diagnostic test, it is put into a Disabled state. The channel must pass the same diagnostic test before it is put into the Off Duty state. Once the channel is in Off Duty state you can return it to the Idle state. Refer to the diagnostic test results for instructions on how to fix the channel. You can view the diagnostic test results through the Diagnostic pane of the Maintenance program.

If a channel is placed in a Disabled state as the result of a hardware problem, the hardware problem must be corrected before the channel is put into the Off Duty state. Once the channel is in Off Duty state you can return it to the Idle state. Run diagnostic tests on the channel from the Maintenance program to determine the cause of the problem. After the problem is corrected, rerun diagnostics to ensure that the channel is operational.

Once the problem has been corrected, the channel must be restarted, as outlined in [“To start multimedia channels” on page 374](#).

Viewing multimedia channel states

Introduction

You can view the state of all multimedia channels using the Multimedia Channels window. From this window, you can monitor the current activity of functioning channels.

If the server experiences trouble with processing incoming calls, you can view the state of all multimedia channels simultaneously in the Multimedia Monitor window on the client to determine whether

- channels are out of service or disabled
- there is an imbalance in the distribution of calls being received (for example, voice channels might be busy while fax and speech recognition channels remain idle)

If channels are Off Duty, use the Hardware maintenance utility to diagnose the problem.

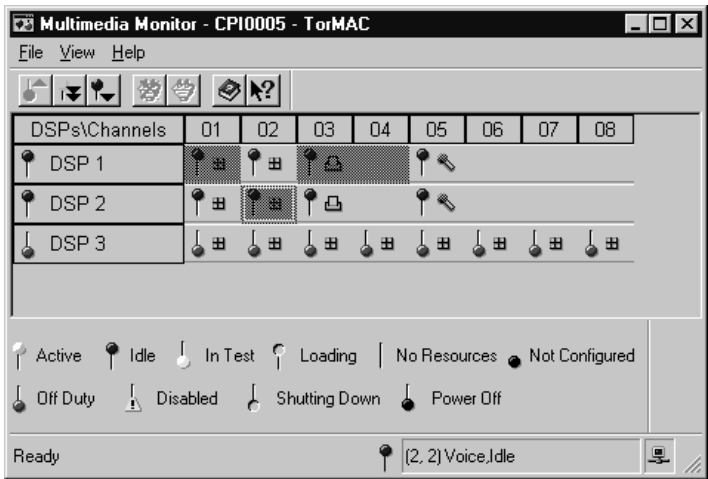
If users are complaining that lines are busy, the distribution of calls over the existing channels might not be balanced. This imbalance can occur if the system does not have the optimum distribution of voice, fax, and speech recognition channels. For example, if the system is not receiving many fax calls, there might be some idle fax channels. At the same time, the voice channels might be overloaded. Fax or speech recognition channels can be reassigned to another function to temporarily relieve an imbalance in the distribution of calls.

Getting there CallPilot System > System Administration > Maintenance Administration > Multimedia Monitor

To view multimedia channels

- 1 Double-click Multimedia Monitor.

Result: The Multimedia Monitor window appears showing the state of all multimedia channels.



Refresh rate

By default, the Multimedia Monitor window refreshes every five seconds. Any changes in the state of a multimedia channel are shown.

You can change the rate at which the Multimedia Monitor window is refreshed to one second or two seconds if you require more frequent updates.

Note: When you increase the refresh rate, you increase the load on the server, because this increases the traffic between the server and the client.

To change the refresh rate

- 1 In the Multimedia Monitor window, click View > Refresh Rate.
- 2 Select one of the following:
 - 1 sec.
 - 2 sec.
 - 5 sec.

Viewing multimedia channel media types

Introduction

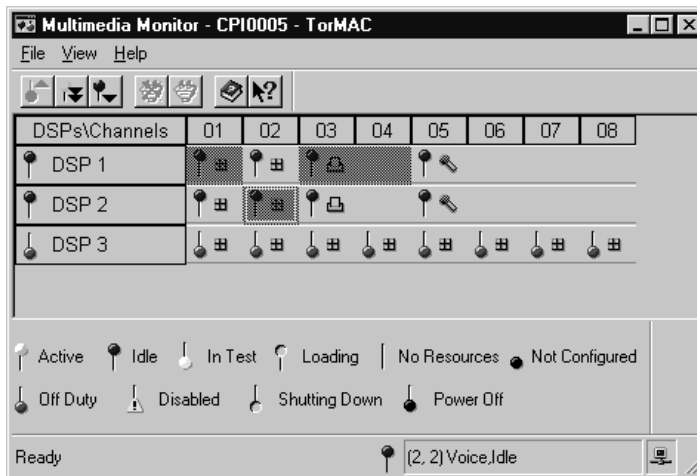
You can view the media type of all multimedia channels on the Multimedia Monitor window. From this window, you can see whether channels are configured as voice, fax, or speech recognition. This can help you determine whether you need to reconfigure the channels or add MPC-8 cards to increase the multimedia processing capacity of the server.

Getting there CallPilot System > System Administration > Maintenance Administration > Multimedia Monitor

To view multimedia channel media types

- 1 Double-click Multimedia Monitor.

Result: The Multimedia Monitor window appears showing the media types of all multimedia channels.



Powering multimedia channels on and off

Introduction

If it is necessary to replace or install a new MPC-8 card or MPB-16 board, you must power down the channels for the associated card through the Multimedia Monitor window.

Once the new hardware has been installed, or the diagnostics have been completed, you must power up, then restart the channels.

Note: The on-screen power buttons are not currently available on some servers.

Powering down the multimedia channel

If you need to take a channel or card out of service to perform an upgrade or maintenance, you must first stop the channels and remove power.

- 1 Highlight the channels or cards that are to be removed from service on the Multimedia Monitor window.
- 2 Perform a Courtesy Stop or Stop to take those channels out of service, as outlined in [“Stopping multimedia channels” on page 375](#).
- 3 Click Power Down on the toolbar to stop the electrical current from reaching the selected card(s).
- 4 Remove the MPB-16 board to perform the necessary maintenance or upgrade.

Powering up the multimedia channel

Once the required maintenance has been completed, or the new hardware has been installed, you must power up the associated board and restart the channels.

- 1** Highlight the board that was removed from service.
- 2** Click Power Up on the toolbar to allow the electrical current to reach the selected card(s).
- 3** Select File > Start Channels, or click Start on the toolbar to start the selected channels.
- 4** Wait a few seconds for the channel state to be updated.
- 5** Verify that the selected multimedia channels have changed status to Idle (or Active).

Starting and stopping multimedia channels

Introduction

The following procedures are performed from the Multimedia Monitor.

Getting there CallPilot System > System Administration > Maintenance
Administration > Multimedia Monitor

Starting multimedia channels

Introduction

After diagnostics, upgrades, or installations have been completed, or problems with an unhealthy channel have been resolved, you must start the channel to put it back into service.

When a channel is started, the state of the channel is changed from Off Duty to Idle to wait for voice, fax, or speech recognition data to transport from the switch to the server.

You can stop and start an individual multimedia channel, more than one multimedia channel, or all multimedia channels in the Start/Stop Channels window. Only Off Duty channels can be started.

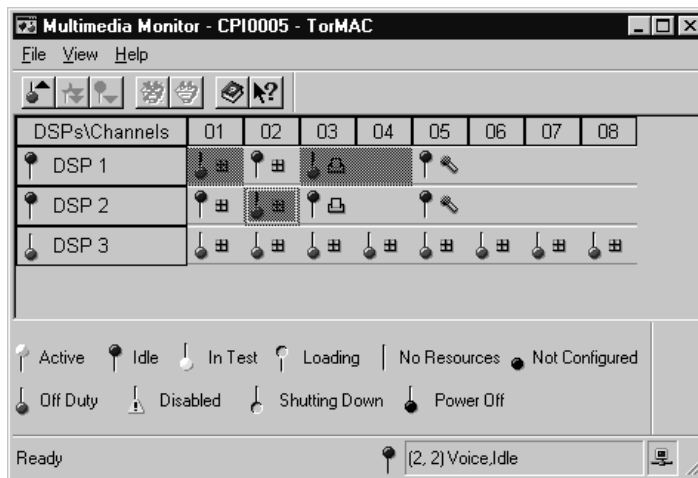
Note: You can also start and stop individual multimedia channels from the Maintenance tab of the Hardware Maintenance window.

When to start channels

Typically, you start multimedia channels after the system has been powered up following an upgrade or installation, or after a diagnostic has been completed. You should also start Off Duty channels as soon as they are ready to be operational again. This enables the channels to process call data again.

To start multimedia channels

- 1 From the Multimedia Monitor window, select the individual channel or range of channels that you wish to start, as follows:
 - To select all channels in the system, click the Channels type heading on the top left corner of the channels chart.
 - To select all channels for a particular card, click the card button in the left column.
 - To select a specific number channel, click the multimedia channel number heading (for example, 04).
- 2 Select File > Start Channels, or click Start on the toolbar to start the selected channels.



- 3 Wait a few seconds for the channel state to be updated.
- 4 Verify that the selected multimedia channels have changed status to Idle (or Active).

Stopping multimedia channels

Introduction

Stop multimedia channels to take healthy channels and cards out of service before performing diagnostics, upgrades, or installations, or if there is a problem with a channel or the system. When you stop a channel, it is placed on Off Duty status. While in this state, the multimedia channel cannot carry any voice, fax, or speech recognition data from the switch to the server.

You can stop and start an individual multimedia channel, more than one multimedia channel, or all multimedia channels in the Start/Stop Channels window. Only Active or Idle multimedia channels can be stopped.

Note: You can also start and stop individual multimedia channels from the Maintenance tab of the Hardware Maintenance window.

Methods of stopping

There are two methods that can be used to stop a channel: stop or courtesy stop.

- **Stop**

A stop puts an Active or Idle multimedia channel or card into Off Duty status immediately, even if it is busy processing call data. All calls using these channels are disconnected. Use a stop only when severe problems occur that are affecting a large number of calls or if your organization determines a special need for it.

- **Courtesy stop**

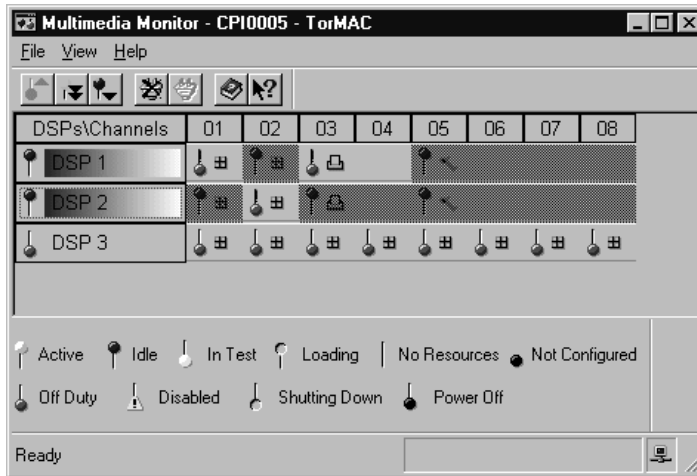
A courtesy stop waits until all call data has been processed before putting active or idle channels into Off Duty status. No calls using these channels are interrupted.

Typically, you courtesy stop multimedia channels before performing diagnostics, upgrades, or installations.

To stop multimedia channels

- 1 From the Multimedia Monitor window, select the individual channel, card, or range of channels that you wish to stop, as follows:
 - To select all channels in the system, click the Channels type heading on the top left corner of the channels chart.

- To select all channels for a particular card, click the card name in the left column.
 - To select a specific channel number, click the multimedia channel number heading (for example, 04).
- 2 Determine whether you want to perform a courtesy stop or stop. Refer to [“Methods of stopping” on page 357](#) for an explanation of the difference.
 - 3 Select File > Courtesy Stop or File > Stop, or click Courtesy Stop or Stop on the toolbar to stop the selected channels.



- 4 Wait a few seconds for the channel state to be updated.
- 5 Verify that the selected multimedia channels have changed status to Off Duty.

Chapter 13

Troubleshooting

In this chapter

Overview	378
Section A: Outcalling services	379
Types of problems users might encounter	380
Events generated by Outcalling services	385
Using Reporter to monitor and troubleshoot Outcalling services	388
Section B: System operation problems	391
Overview	392
Troubleshooting checklist	393
Troubleshooting examples	396

Overview

Introduction

This chapter contains information and suggestions on troubleshooting call service and system operation problems.

For hardware troubleshooting information, see the *Installation and Configuration Guide* applicable to your server.

Section A: Outcalling services

In this section

Types of problems users might encounter	380
Events generated by Outcalling services	385
Using Reporter to monitor and troubleshoot Outcalling services	388

Types of problems users might encounter

Introduction

This section describes how to troubleshoot problems in Remote Notification, Delivery to Telephone, and Delivery to Fax once these services have been put into service.

The types of problems that can occur when using Outcalling services include

- being unable to use the Outcalling service because channels are not available
- experiencing a high rate of failures because of incorrect configuration or the retry limits are exceeded

Unable to place outcalls

Symptoms

Outcalling services are not able to obtain channels to place outgoing outcalls.

Causes

The channel allocation might not be spread evenly, or channels might be out of service or faulty.

What to do

- Check channel allocations.
- View channel states.
- Generate and review reports.

Check the channel allocation

A setting of 0 for the minimum number of channels means that no channels are guaranteed to the service. If the system is very busy and there is a request for an outcall, there might not be sufficient channel resources to handle the call.

To manage channel usage, the maximum number of channels puts a limit on how many channels a service can use at any one time. The default of a two-channel maximum is sufficient for average use. However, if one or more of your Outcalling services is heavily used, consider increasing the minimum and maximum channel allocations.

To check the channel allocation, see

- “Accessing the Service Directory Number Table” in the *Administrator’s Guide*
- “Configuring an outbound Service DN” in the *Administrator’s Guide*

Check the status of channels

The states in the following table indicate the current activity or status of each call or multimedia channel.

Channel state	Description
Active	The channel is working and currently transporting call data from the switch to the server.
Idle	The channel is working but not currently transporting call data from the switch to the server.
In Test	The channel is undergoing diagnostic testing.
Loading	The channel has been started, which takes it out of the Off Duty state. This state occurs quickly and is immediately followed by the Idle state.
No Resources	The hardware required for channels to operate is not installed or not operating properly.
Not Configured	The hardware has been installed, but the channel has not been properly configured.

Channel state	Description
Remote (Yellow) Alarm	(Call channels only) A yellow alarm is sent by the receiving T-1 device to the transmitter device. It indicates to the transmitter device that a red alarm condition exists at the receiver device. The yellow alarm is sent for as long as the red alarm condition exists at the receiver device.
Off Duty	The channel has been stopped. The channel might have stopped as the result of a problem with the channel, a problem with a parent component, or someone taking the channel off duty.
Remote Off Duty	(Call channels only) The channel was taken out of service at the switch.
Disabled	The channel has been disabled, perhaps as the result of a failed diagnostic or hardware failure.
Shutting Down	The channel has been stopped. This state occurs quickly and is immediately followed by the Off Duty state.
Power Off	The electrical current has been turned off to the selected card.
Local (Red) Alarm	(Call channels only) A red alarm condition occurs when Receive Loss of Synchronization (RLOS) has existed for 2.5 seconds (default) on incoming data. This condition exists until the synchronization has been recovered and remains recovered for 12 seconds (default).

To view channel status, see

- [“Viewing call channel states” on page 352](#)
- [“Viewing multimedia channel states” on page 367](#)

Generate and review reports

Outcalling reports are useful in determining how much particular services are being used and whether outcalling services are able to acquire the needed channel resources.

The following reports might also prove useful:

- Service Quality Summary report
- Service Quality Detail report
- Channel Usage report
- System Traffic Summary

For information about these reports, see the *Reporter Guide*.

DTT or DTF delivery failures

Symptom

There is a high rate of delivery failures.

Causes

The following conditions might prevent a DTT or DTF message from being successfully delivered:

- busy
- no answer
- answered, but no DTMF confirmation was provided or the call was terminated before delivery can take place

Check the retry strategy

The retry strategy consists of a retry interval and a retry limit for each of the three conditions. When a delivery attempt is unsuccessful, the retry strategy is checked to see how often retries should be attempted (the interval) and up to how many times (the limit). The first attempt is not counted, since it is not a retry.

For instructions, see

- “Configuring Delivery to Telephone and Delivery to Fax for a user group” in the *Administrator’s Guide*

Generate and review reports

The following reports might be useful in detecting problems:

- DTT Activity report
- Fax Deliveries Activity report

Remote notification failures

Symptoms

There is a high number of failed Remote Notification requests or other failures, or both.

Causes

These are some possible causes:

- The users' Remote Notification target DNs are restricted.
- User pager setups might not be correctly configured.
- Retry limits were exceeded.

Check and review report

Run the RN Activity Report to help detect the problem. For instructions on running the report and performing troubleshooting, see the *Reporter Guide*.

Events generated by Outcalling services

Introduction

This topic identifies the events that are generated when problems are experienced by Outcalling services. While investigating these events, review previous events to determine the cause of the error. If you are not able to determine the cause of the problem, contact your support organization.

Common events

The following events are common to Remote Notification, Delivery to Telephone, and Delivery to Fax problems:

Event code	Description
59500	System Error in the Outcalling Application.
59501	Invalid Application ID for Outcalling.
59532	Unable to Access Profile Information for Remote Notification Session.

Delivery to Telephone and Delivery to Fax events

The following events are generated for both Delivery to Telephone and Delivery to Fax problems:

Event code	Description
59512	Internal Error. Unable to Find Message for Delivery in MTA Mailbox.
59513	Internal Error. Sender Address missing in MTA Message for Delivery.
59514	Unable to Register with Message Transfer Agent.

Event code	Description
59515	Unable to Deregister with Message Transfer Agent.
59516	Unable to Send Connection Info to Message Transfer Agent.

Remote Notification events

The following events are generated for Remote Notification problems:

Event code	Description
59529	Unable to record Outcalling Parameters in WinNT Registry.
59530	Unable to record Outcalling Parameters in WinNT Registry.
59531	Unable to Deregister with Notification Server.
59533	Unable to Access Mailbox Information for Remote Notification Session.
59534	Unable to Access Message Information for Remote Notification Session.
59535	Unable to Lock Profile Information for Remote Notification Session.
59536	Unable to Update Profile Information for Remote Notification Session.

Remote Notification server events

The following events are generated for Remote Notification server problems:

Event code	Description
55076	The remote notification outgoing agent failed to send out a remote notification to a user.

Event code	Description
55077	Remote Notification Outgoing Agent failed to register within the timeout limit.
55078	Remote Notification Agent failed to deregister within the timeout limit.
55079	User RN data retrieval error. This is likely due to database not ready to accept request yet.
55081	Failed to add a recovery record to the database. This is likely due to database not ready to accept request yet.
55082	Failed to delete a recovery record from the database. This is likely due to database not ready to accept request yet.

Using Reporter to monitor and troubleshoot Outcalling services

Introduction

You can generate a number of reports in Reporter to help you analyze Outcalling usage and to troubleshoot problems with Outcalling services.

The reports

The following table identifies the Outcalling reports you can generate:

Report name	Description
RN Activity Report	Provides information about Remote Notification activity during a specified time period. It is helpful for determining RN busy times.
RN Audit Trail Summary Report	Helps you determine which RN attempts are responsible for the high number of failures detected by the RN Activity Report.
RN Audit Trail Detail Report	Provides details of each request submitted to the RN service. This report is typically run after the RN Audit Trail Summary Report.
Fax Deliveries Activity Report	Monitors Delivery to Fax and fax printing activity over a specified time period. This report helps you to determine how much the services are being used, whether the DTF service is able to acquire channels when needed, and whether the DTF retry settings are adequate.

Report name	Description
Fax on Demand Audit Trail Summary Report	Provides summary information about DTF calls placed by Application builder services with fax callback capability. This report is used to troubleshoot problems with an Application Builder service or particular fax device, and the cause of lengthy fax delivery sessions.
Fax on Demand Audit Trail Detail Report	Helps you to determine why a specific fax delivery attempt has failed by enabling you to trace the fax delivery process from the outcall request to the final outcome.
Fax Print Audit Trail Summary Report	Provides summary information about fax printing. Use this report to troubleshoot problems with fax machines and associated mailboxes that have high retry counts and failures.
Fax Print Audit Trail Detail Report	Helps you determine why a specific fax print delivery attempt failed. Use it to trace the fax delivery process from the print request to the final outcome.

Generating the reports

Report generation consists of the following major steps. These steps are explained in more detail in the *Reporter Guide*.

To generate reports

- 1 Collect and download Traffic OMs from the CallPilot server.
For instructions, see the “Setting up Operational Measurements (OMs) for Reporter” chapter in the *Reporter Guide*.

- 2 Add the reports you need to Reporter.

For instructions, see the “Generating reports” section in the *Reporter Guide*.

Note: For instructions on customizing the reports, see the “Customizing the data displayed in reports” section in the *Reporter Guide*.

- 3 Print and export the report.

For instructions, see the “Printing and exporting reports” section in the *Reporter Guide*.

- 4 Review the reports.

For troubleshooting instructions, refer to the description for each report in the *Reporter Guide*.

Section B: System operation problems

In this section

_Overview	392
_Troubleshooting checklist	393
_Troubleshooting examples	396

Overview

Introduction

This section provides solutions for operation problems you might encounter with your CallPilot system.

Problems you might encounter with a specific feature of CallPilot (for example, Application Builder, Reporter, Desktop Messaging, or Networking) are not provided in this section. Refer to the specific guide for help with troubleshooting these types of problems.

Troubleshooting checklist

Introduction

This section lists some problems that can occur on your system, and the appropriate troubleshooting steps.

Alarms occurring despite no apparent system problem

If the system shows no apparent system problem but alarms are occurring, check if someone has recently run diagnostics on the system. A diagnostic test can generate an alarm as part of its test even if the system is fine.

Performance problems

Calls not being answered

- If CallPilot is improperly configured, you can get errors such as calls not being answered. If you receive complaints about system performance, and you fail to detect a hardware problem, check the CallPilot configuration.
- If calls are unanswered (ringing but no answer), check that the Service DN table is configured properly. Also check that the caller is dialing the correct DN. If a caller is dialing a DN that is not listed in the Service DN table, then the call is not answered.

If the Service DN is configured correctly and the caller is dialing the correct DN, then you must check the Alarm monitor, the Multimedia Channels window, and possibly the Maintenance Window to look for the cause of the problem. Refer to [“Troubleshooting examples” on page 396](#) for an example of this scenario.

Call flow from the switch is impaired

If the switch is improperly configured, this affects the call flow from the switch to the server and can result in a performance problem.

Call answered, but no prompts are heard

If the system answers calls but does not supply any prompts, then pursue the following possibilities:

- Check if there is an error in the application that supports the requested service. If an error exists, it might be preventing the prompts from playing.
- Observe the Multimedia channels and DSO channels windows to see if the channels are going from idle to active as a call comes in. If DSO channels are remaining idle, then the problem is with the DSO channels. If all DSO channels on a single DS30x link are remaining idle as calls come in, then the cable link might be disconnected, or connected to the wrong connector.

Refer to the [“Troubleshooting examples” on page 396](#) for an example of this scenario.

System is not working after a change in IP address

If the IP address of a CallPilot server is changed while the system is up and running, the system will not work until you restart the switch.

If you want to change the IP address of the CallPilot server, use the following procedure.

To change the IP address

- 1 Shut down the telephony service.
- 2 Change the IP address. The change becomes effective on the switch immediately.
- 3 Restart the CallPilot server to bring the system back to normal service. This starts the telephony service and the CallPilot applications.

System monitor shows a blue screen

If the system monitor suddenly shows a blue screen with just white text on it, a system error has occurred. Write down all the events that took place prior to the blue screen appearing. Then write down any text that appears on the blue screen and contact customer support for assistance.

The text on the blue screen usually begins with “*** STOP:”. The relevant information that might appear is explained in the following subsections.

STOP code section

The stop code section contains an eight hexadecimal digit STOP code, four eight hexadecimal digit STOP code parameters, and a single line of text (the second line) identifying the device driver and/or address that caused the system error.

For example:

```
*** STOP: 0x0000000A (0x00000000, 0x00000002,  
0x00000000, 0xFCE10796)  
  
IRQL_NOT_LESS_OR_EQUAL*** Address fce10796 has base at  
fce10000 - NTbus.sys
```

Stack trace section

The stack trace section contains a list of function calls on the stack that preceded the system error.

Only the right-most column of the stack trace is important; it identifies the device drivers that were being called at the time of the error.

For example:

```
Address dword dump Build [1314] - Name  
  
f416d18 fce10796 fce10796 ff4f9c10 e1304018  
801862e3 00000246 - NTbus.sys  
  
ff473902 fc483650 fc538353 ff62f827 e8836502  
8386502d 03850h59 - ntoskrnl.exe
```

Recovery instructions section

Every time a blue screen is generated, a dump of physical memory is written to the d:\Winnt\MEMORY.DMP file. The recovery text on the blue screen indicates when this writing operation has completed and therefore, when it is safe to restart the system.

For example:

```
Beginning dump of physical memory.  
Physical memory dump complete. Contact your system  
administrator or technical support group.
```

Note: Do not restart until the recovery section indicates that the physical memory dump is complete.

Troubleshooting examples

Introduction

This section provides examples of what troubleshooting steps you can take to solve system problems.

This section focuses on two example problems and the steps to solve these problems.

Call unanswered

The scenario

A user calls a DN assigned to a particular service. There is ringing, but the call is not answered. The user lets the phone ring long enough to be directed to whatever service is in place (for example, an auto attendant), but the phone continues to ring with no answer.

To troubleshoot

- 1 Check that the Service DN table is configured properly and that the caller is dialing the correct DN.

Example: If a caller is dialing a Service DN from a phone but the Service DN has been configured for fax, then the call is not answered. A Fax Service DN accepts calls only from fax machines.

If the Service DN is configured correctly and the caller is dialing the correct DN, you need to do additional troubleshooting. See steps [2](#) to [9](#).

- 2 Check the Alarm Monitor window for any alarms with event ID 38007. This Event ID is for DSP or channel alarms. These alarms can be related to the current problem. Double click on the alarm to obtain the online Help information for the alarm. If this does not lead to a solution, continue with the next step.
- 3 Check for alarms indicating that a service is not running. If this type of alarm is found, check that the service that is being requested on CallPilot is operational and in service. If the requested service is in service, then continue with the next step.

- 4 Open the Multimedia Monitor window on the CallPilot Administration Client window.
- 5 Observe the state of the multimedia channels. Then do one of the following substeps:
 - a. If all multimedia channels on an MPC-8 card are Off Duty, go to step [6](#).
 - b. If all multimedia channels are in service (Idle or Active), go to step [6](#).
 - c. If only some multimedia channels on an MPC-8 card are Off Duty, attempt to Start those channels. If the channels do not start, go to step [6](#).
- 6 Open the Maintenance Window.
- 7 Do one of the following substeps:
 - a. If the MPC-8 cards are in service, check the switch configuration.
 - b. If an MPC-8 card is Off Duty, start the MPC-8 card. If the MPC-8 card and its multimedia channels do not start, then run diagnostics on the MPC-8 card. After running diagnostics, attempt to start the MPC-8 card again.
- 8 If the problem persists, restart the server if possible.
- 9 If the problem persists, call customer support.

Call answered, but no prompts are heard

The scenario

A user calls a DN assigned to a particular service. The call is answered, but no prompts are heard.

To troubleshoot

- 1 Check if there is an error in the application that supports the requested service. If an error exists, it might be preventing the prompts from playing. If the application is working properly, continue with the next step.
- 2 Open the Multimedia Monitor window and the Channels Monitor window on the CallPilot Administration Client.
- 3 Make several calls into the system to try to make each DSO channel go active.

- 4** Observe the states of the multimedia and DSO channels as you make each call.
- 5** If a multimedia channel goes active as you make a call but the DSO channel remains idle, then the problem is with the DSO channel. Do one of the following substeps:
 - a.** If all DSO channels on a DS30x link remain idle as you put in calls to the system, the link might be broken between the switch and the server. Check that the DS30x link cable is connected to the appropriate connectors on the switch and the server. If the cable is connected properly and the problem persists, go to step [6](#).
 - b.** If only some of the DSO channels are not responding to the calls (remaining idle as the call comes in), then stop and then start those channels. If the problem persists, then go to step [6](#).
- 6** If the problem persists, restart the server if possible.
- 7** If the problem still persists, restart the switch if possible.
- 8** If steps 6 or 7 do not fix the problem, contact customer support.

Part 3

Securing the CallPilot system

In this part

Chapter 14: Introduction to CallPilot security	401
Chapter 15: Physically securing your equipment and data	415
Chapter 16: Maintaining system password security	421
Chapter 17: Implementing CallPilot security features	431
Chapter 18: Monitoring and auditing CallPilot system activity	441
Chapter 19: Using Hacker Monitoring	459
Chapter 20: Security features on the Meridian 1 switch	483

Chapter 14

Introduction to CallPilot security

In this chapter

Overview	402
Security strategies	404
Common hacker techniques	406
Security threats to messaging systems	408
How to protect CallPilot	410

Overview

Introduction

This chapter describes the types of security threats to CallPilot, both intentional and unintentional, and the methods that are used to get into messaging systems. The other chapters in this part explain how to protect your system against these threats.

Many consequences result from a lack of good security policies and measures. Some possible consequences include nuisances such as hackers leaving users obscene messages. More serious breaches include service interruptions, deleted files, viruses, stolen passwords and information, and costly telephone bills due to unauthorized long-distance calls.

Types of security threats

Threats to voice and data security fall into the following broad categories:

- Lack of physical security of equipment. This includes not keeping equipment safe from intentional and unintentional damage.
- Theft of information. This includes sensitive information, access codes, and passwords.
- Unauthorized use of services. For example, unauthorized system users might place long-distance calls and incur toll charges against your switch.
- Information leaks. Employees can unknowingly provide information or access to equipment or services to people posing as other employees or technicians.

Intentional and unintentional security breaches

Security breaches can be intentional or unintentional. The emphasis is usually on criminal activity. However, a security policy should also consider how equipment or data can be unintentionally damaged or how information can accidentally get into the wrong hands.

Anything that presents a danger to your network, such as a hard drive failure or a fire, is a security threat. To prevent unintentional security breaches, you should educate your employees about the risks and how to deal with them and having disaster recovery plans in place for problems that cannot be prevented.

Legal responsibility

Normally, the courts consider companies that use devices such as Private Branch Exchanges (PBXs) and messaging systems that are connected to the public switched telephone network (PSTN) responsible for calls that originate from their telephone systems. This means that courts consider companies responsible for the security of their systems.

Security strategies

Introduction

CallPilot is a sophisticated messaging system. Its many features can greatly enhance and facilitate communications in your organization. Since CallPilot is essentially a computer that resides on a network, it can become the target of abuse just like any other computer.

No single answer works for all businesses. The chapters in this part help you to find the security answers that are right for your organization. To decide on an appropriate security solution, you must complete the following actions.

Familiarize yourself with the risks and threats

Read the chapters in this part to better understand the security risks to messaging systems.

Read books and magazines and visit security-related web sites to keep up to date on the latest techniques that hackers are using. For example, Microsoft has an excellent site with informative articles about Windows NT security issues.

Develop a security policy

Call together the appropriate people in your organization to discuss a security policy. People who are experts in your business and its priorities and security experts need to work together to strike a balance among security and cost, business needs, and convenience.

Layer security measures throughout your network

Use all of the security features in CallPilot, the server, and the switch to maximize the security of your system. Protect your network with whatever hardware and software solutions you consider necessary. This can include implementing firewalls, using Windows NT security features, securing remote access modems, or whatever additional security measures are needed to meet the level of security required by your business.

Monitor your system regularly

One of the main causes of security breaches is that system activity is not monitored regularly. Therefore, establish a baseline of activity for your system so that you can identify what is normal. Only then can you notice abnormal activity and be able to act quickly.

Common hacker techniques

Introduction

Familiarize yourself with the methods used to break into messaging systems to help you understand how to maximize CallPilot security.

How hackers log on to messaging systems

To gain access to a system, a hacker has to identify a number of access codes: the telephone number that gives an external caller access to the messaging system, a valid mailbox number, and the password for a mailbox.

A valid access code can be obtained manually, using a telephone. The hacker dials number after number until he or she finds a valid access code. However, a program called a demon dialer or war dialer does the dialing much more rapidly. War dialers can be set up to dial numbers randomly, sequentially, or by using an algorithm.

How hackers get information about your company

Rather than trying to guess valid access numbers, hackers might try to obtain actual numbers and passwords. They use the following techniques to gather information.

Dumpster diving

Hackers go through a company's garbage looking for printouts and records that contain system information such as phone numbers, mailbox numbers, and passwords.

Ensure that this type of information is properly disposed of. Shred all printouts containing this kind of information before throwing them out. While printouts containing this information are in use, keep them locked up.

Social engineering

Social engineering is the practice of getting a corporation's information by pretending to be an authorized technician, supplier, or employee.

Make it a policy for employees to ask for identification whenever a strange or suspicious person is seen in the building, or when someone calls and asks for company information.

Security threats to messaging systems

Toll fraud: Unauthorized long distance calls

Telephone systems such as switches and messaging systems are vulnerable to toll fraud if not properly secured. Toll fraud occurs when someone gains unauthorized access to a telephone system and uses it to place long distance or international calls free of charge. Since these calls originate from your switch, charges are billed to your company. Access to thru-dialing capabilities is one of the main reasons hackers attack messaging systems.

Several CallPilot features provide thru-dialing and outcalling capability. It is important to apply the appropriate dialing restrictions to these features.

Illicit mailboxes

Hackers who gain access to messaging systems sometimes set up their own mailboxes. They use these mailboxes to exchange information or to gain regular access to features. Hackers try to find unused mailboxes to take them over. This is why it is so important to find and delete all unused mailboxes.

Changed greetings and obscene messages

Hackers sometimes carry out pranks. For example, they might leave humorous or obscene messages for users. Or, they might change mailbox users' personal greetings (such as personal verifications).

It is more serious when hackers gain access to administrative features that allow them to change system greetings or greetings used in Application Builder services. Thus it is crucial to make administrators' accounts even more secure.

Fax callback services

Hackers can gain access to a service that provides fax callback service. With this type of service, callers dial a number and are given an option to have a fax transmitted to a callback number entered by the caller.

If long distance callback numbers are allowed, hackers might request long faxes to be sent to numbers that are really pay-per-call numbers.

How to protect CallPilot

Introduction

The rest of the chapters in this part describe in detail what you can do to make CallPilot as secure as possible. Here is a summary of the most important actions you can take and references to the relevant chapters.

Built-in security features

A few security features are automatically enabled and do not require any setup.

- Password suppression
This feature prevents the passwords that users enter on their telephone keypads from displaying. Instead of displaying the numbers, a series of asterisks is displayed. This makes it difficult for shoulder surfers to identify passwords. Note that the availability of this feature depends on the release of X11 software you are running.
- Trivial passwords
This feature prevents users from defining very obvious mailbox passwords, such as 0000 or 1234. Users are prompted to enter a different password when they try to define a trivial password.

Secure administrators' accounts

Administrators have access to parts of the CallPilot system so that they can administer it. For example, anyone who needs to create services in Application Builder or to modify users must be added to the system as a user with administrative capabilities.

Since administrators can modify the system configuration, decide who has access to which parts of the system. Access classes allow you to define access rights (read only, read and write, and so on) for each object in the system management interface. Once access classes are defined, assign each administrative user to a particular class to control what each administrator can and cannot do.

See also

For more information about creating access classes, see “Setting up access classes for administrative users” in the *Administrator’s Guide*.

Protect services that dial out

Several CallPilot services are capable of dialing out to the public network. If you do not put dialing restrictions on these services, hackers might use them to place long distance calls. Features in CallPilot and on the switch are used to restrict the numbers that can be called:

- restriction/permission lists (CallPilot)
- Trunk Group Access Restrictions (TGARs), Class of Service (CLS), and Network Class of Service (NCOS) on the switch

Default settings provide maximum security

By default, on any newly installed system, all CallPilot services that can dial out of the system are completely restricted. This means that these services will not work until you define restriction/permission lists and assign them to services. This ensures that you consider each feature and implement a policy about the numbers you want to restrict and permit for each.

See also

For more information on defining restriction/permission lists and applying them to features, see “Setting up restriction/permission lists” in the *Administrator’s Guide*.

For more information on using switch features such as TGAR, CLS, and NCOS, see [Chapter 20, “Security features on the Meridian 1 switch.”](#)

Secure users’ mailboxes

Hackers try to find mailboxes that they can log on to. Mailbox passwords that are hard to guess make your system more secure. If a hacker cannot guess a password, he or she cannot get into a mailbox.

Hackers look for unused mailboxes that are still active on the system (for example, mailboxes of employees who have left the company but have not been deleted from the system). Be sure to delete mailboxes as soon as employees leave your company. Check for unused mailboxes regularly.

See also

For more information on how to make mailboxes and passwords as secure as possible, see [“Secure users’ mailboxes” on page 439](#).

Change default greetings and prompts

When a hacker gets through to a messaging service, the first thing he or she hears is a system greeting that either identifies the type of messaging system or the organization.

By default, the CallPilot system greeting is “CallPilot.” For security reasons, it is recommended that you change this greeting and use it to identify your organization. If the greeting identifies the type of messaging system, hackers immediately know which system they are dealing with. They can get instructions on how to use the system from other hackers.

Several prompts identify the system type as CallPilot in the default version of the prompt.

See also

For more information about customizing system prompts and greetings, see “Customizing prompts, greetings, and faxes” in the *Administrator’s Guide*.

Secure your LAN

CallPilot resides on your corporate LAN. In addition to protecting your system from the security threats common to messaging systems, you must protect it from the threats of networked systems, especially if you are connected to the Internet. Consult a network security expert to discuss possible problems and appropriate solutions.

Monitor your system regularly

Generate and analyze Reporter reports regularly. These reports allow you to view and analyze useful OMs that tell you how your system is being used. You first need to establish a baseline of normal activity for your system. Monitor relevant reports regularly so that you notice unusual patterns as soon as possible.

See also

For more information on monitoring, see [Chapter 9, “Viewing and filtering server events.”](#)

Use Hacker Monitor to track suspicious activity

If you suspect that hackers have gained access to your system, enable Hacker Monitor. You can monitor your system for accesses to and thru-dials from suspected mailboxes. Or, you can monitor calls made by specific caller line IDs (CLIDs) that you suspect hackers are calling from. You can also monitor thru-dials made by services you have created with Application Builder.

You are notified of monitored events in real time, as they occur. This is because alarms and events are generated that can be viewed in Event Browser or Alarms Monitor. To receive automatic notification of these events, you can set up an alarm mailbox so that the system sends you a message as soon as an event is triggered by Hacker Monitor.

See also

For more information, see [Chapter 19, “Using Hacker Monitoring.”](#)

Secure your Web Messaging system

For information on security for the CallPilot Web Messaging system, see the *Desktop Messaging Installation and Maintenance Guide*.

Chapter 15

Physically securing your equipment and data

In this chapter

Overview	416
Securing the premises	417
Securing equipment	418
Disposing of printed information	420

Overview

Introduction

This chapter describes some of the measures to take to make your work environment, equipment, and printed data more secure.

Securing the premises

Introduction

Physical security threats include things that can physically damage equipment, as well as ways in which equipment can be physically accessed to get to information. When considering physical security, think not only of network media such as cabling and servers but also of clients and laptops.

Guidelines

Here are some guidelines for increasing the security of your workplace:

- Do not let visitors roam freely.
- If tours of the office are conducted, make sure employees are aware of them. Sensitive data must not be left on computer screens or desktops.
- When people claim they are contractors or technicians, ask for identification. Verify that they are supposed to be there.
- Decide on a policy for after-hours access to your facilities, and educate employees. Do not leave it up to employees to decide who can come in and when.

Securing equipment

Introduction

Set up a security policy to identify the measures that are put into place to secure equipment.

The equipment room

Try to keep all servers and other critical equipment in a room (or rooms) that can be locked. If an equipment room is used for several purposes, consider separate rooms. Here are more guidelines for securing equipment rooms:

- Give only authorized personnel access to equipment rooms. Security badges and a badge reader that records the time and identity of each person entering the room are highly recommended.
- If the equipment room has ceiling tiles, ask your building's maintenance company to secure them or extend the wall through the ceiling.
- Keep track of keys or badges that are used to gain entry. When employees leave your company, cancel the access privileges they had.
- Install hidden video cameras.
- Ensure the room has adequate ventilation and cooling. An overheated room can cause mechanical parts to break down. You can also purchase temperature sensors that page you when the temperature fluctuates a certain amount.
- Do not allow cleaning staff to enter the room. If there is a trash can in the room, set it outside when it gets full. Make sure the can contains no sensitive information.

Cabling and wiring

Cables and wiring present another potential security threat:

- Plan wiring runs, and make them difficult to access.
- Do not leave cabling exposed. Check your premises regularly for loose, exposed, or insecure cabling. Check for cable drops that are inactive, and disconnect them from your hubs until needed.
- Your building's wiring system can be tapped, and electronic emissions can be picked up. Any wiring leading from a computer to the building wiring must be shielded.

Clients and workstations

Client machines and workstations can be vulnerable if not properly protected:

- Use power-on passwords that require a user to enter a password before the system will start. They prevent someone from using a DOS boot disk, inserted in a floppy drive, to bypass the regular boot process.
- Educate users about using passwords and screen savers properly.
- If you give older workstations away or trade in older equipment, be sure to wipe the hard drives with specialized tools. Hard drives that contain sensitive or classified information must be destroyed.

Disposing of printed information

Introduction

Hackers and criminals search through trash (dumpster diving) to obtain useful or sensitive information. Develop a policy for disposing of information and educate employees about it.

Guidelines

Keep important information from ending up in your trash by following these guidelines:

- Identify reports that contain sensitive information, access codes, or passwords. Make sure these reports are shredded.
- You must check file folders that are being thrown out for papers that might have been left in them.
- Shred any network diagrams (that can show where routers are, which ports are blocked, and so on) before throwing them out. While they are still in use, keep these diagrams locked up.

Chapter 16

Maintaining system password security

In this chapter

Overview	422
Changing Nortel Networks user account passwords	423
Changing pcANYWHERE32 passwords	429

Overview

Introduction

To maintain system security, change your server passwords regularly.

For the initial set up of passwords during the installation process, see the *Installation and Configuration Guide* for your server type.

Changing Nortel Networks user account passwords

Introduction

To maintain system security, change passwords regularly and store them in a secure location.

Default accounts and passwords

The following Windows NT accounts are created on the server during the installation procedures at the factory.

Create your own passwords for the Administrator, NGenDist, and NGenDesign accounts (NGenDist and NGenDesign are Remote Access accounts). For the NGenSys account, it is up to your discretion whether to change the default password.

Account	Default password	Intended use
Administrator	abc123	This account has administrative privileges and can be used for configuring the server.
NGenSys	not disclosed for security reasons	An alternate Administrator account
NGenDist	not disclosed for security reasons	Distributor support
NGenDesign	not disclosed for security reasons	Nortel Networks technical support

For more information about these accounts and their passwords, refer to the *Installation and Configuration Guide* for your server type.

ATTENTION

The on-site installer is instructed to change all default passwords as part of the on-site installation procedures. You can change all passwords by using the procedures in this section. Make sure you change all passwords regularly to maintain system security.

If server software is reinstalled, the default accounts and passwords are recreated and passwords must be changed.

When to change passwords

Change passwords at the following times:

- during the initial system setup
- at regular intervals for maximum security
- if you experience trouble logging on to the CallPilot server
- if server software is reinstalled (the default accounts and passwords are recreated, so passwords must be changed)

Note: If you require support from Nortel Networks or your distributor, you must tell them the new passwords.

Password guidelines

Write down any new passwords and store them in a secure place for future reference. Passwords are case-sensitive.

New passwords should be

- unique
- alphanumeric (they should contain at least one number)
- a minimum of six characters
- not nouns

Example

xyd45fst

To change the Administrator password

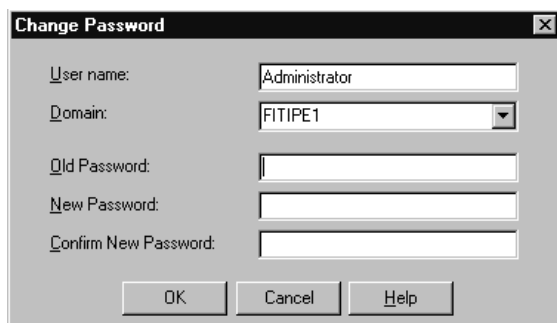
- 1 Log on to the server as Administrator.

- 2 Press Ctrl-Alt-Del.

Result: The Windows NT Security dialog box appears.

- 3 Click Change Password.

Result: The Change Password dialog box appears.



- 4 In the Old Password box, enter the current password.

- 5 In the New Password box, enter the new password.

Note: Ensure the password meets the requirements described in [“Password guidelines” on page 424](#).

- 6 In the Confirm New Password box, enter the new password again.

- 7 Click OK.

Result: A dialog box appears indicating that the password has been successfully changed.

- 8 Click OK.

Result: You return to the Windows NT Security dialog box.

- 9 Click Cancel to close the Windows NT Security dialog box.

- 10 Record the password and store it in a safe, secure place away from the server.

To change the NGenDist and NGenDesign passwords

Note: You are not required to change the NGenSys password. If you change the NGenSys password, you must apply the same password change to the CallPilot Backup/Restore service.

- 1 Log on to the server as Administrator.
- 2 Click Start > Programs > Administrative Tools (Common) > User Manager for Domains.

Result: The User Manager window displays a list of available user accounts, including NGenDist and NGenDesign.

- 3 Double-click the NGenDist icon.

Result: The User Properties window appears.

- 4 In the Password field, type the new password.

Note: Ensure that you use a password that contains a combination of numbers and letters (see [“Password guidelines” on page 424](#)).

- 5 In the Confirm Password field, type the same password entered in the Password field.
- 6 Click OK to close the User Properties window.
- 7 Repeat steps 3 to 6 for NGenDesign.
- 8 Select Exit to save changes.
- 9 Record these passwords and store them in a secure place away from the server.

Note: If you have changed the NGenSys password, continue with the following procedure.

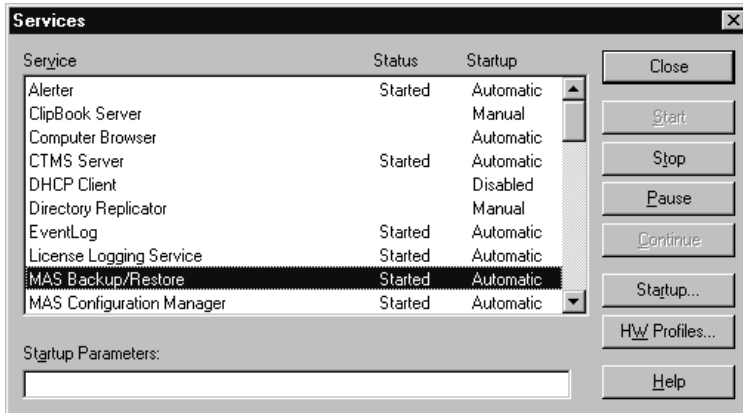
To change the CallPilot Backup and Restore service password to match NGenSys

Note: This procedure is required only if you change the Windows NT user account password for NGenSys.

- 1 Click Start > Settings > Control Panel.

- 2 Double-click Services.

Result: The Services dialog box appears.



- 3 Scroll to MAS Backup/Restore service and select it.

- 4 Click Startup.

Result: The Service dialog box appears.



- 5 In the Log On As section, fill in the Password and Confirm Password boxes with the current NGenSys password.

Note: Use the same password you assigned to NGenSys in ["To change the NGenDist and NGenDesign passwords" on page 426](#).

Changing pcANYWHERE32 passwords

Introduction

During the installation and configuration of pcANYWHERE32, you specify logon passwords. To maintain security, you can change these passwords periodically.

Note: To simplify the remote logon process, Nortel Networks recommends that you match the pcANYWHERE32 caller passwords for NGenDist and NGenDesign to the Nortel Networks user account passwords for NGenDist and NGenDesign. Change the pcANYWHERE32 passwords when you change the Nortel Networks user account passwords for NGenDist and NGenDesign.

To change passwords

- 1 Choose Start > Programs > pcANYWHERE32 > pcANYWHERE.
Result: pcANYWHERE32 starts.
- 2 Select Be a Host PC.
- 3 Click Network.
Note: Do not double-click the icon or you begin a pcANYWHERE32 session.
- 4 Choose File > Properties.
Result: The Network Properties sheet appears.
- 5 Click the Callers tab.
- 6 Click Specify individual caller privileges.
- 7 Right-click the NGenDist icon, and then choose Properties.
- 8 Click the Settings tab.
- 9 In the Password field, type a new NGenDist password.
- 10 In the Confirm Password field, type the NGenDist password again.
- 11 Click Apply.
- 12 Click OK.

- 13** Click the NGenDesign icon.
- 14** Repeat steps [8](#) to [12](#) to create a new password for NGenDesign.
- 15** Click OK to return to the main pcANYWHERE32 window.
- 16** Exit pcANYWHERE32.

Chapter 17

Implementing CallPilot security features

In this chapter

Overview	432
Restrict administrators' access to the system	435
Place dialing restrictions on features	437
Secure users' mailboxes	439

Overview

Introduction

This chapter summarizes the security features available in CallPilot. Detailed setup instructions are given elsewhere (in “Setting up administration” in the *Administrator’s Guide*), as setup is part of the initial system provisioning. Use this chapter as a checklist to make sure you have considered and implemented all CallPilot security features.

CallPilot provides several features that can greatly enhance the security of your system. Make sure you have considered these features in your security policy and that you have configured them to meet your organization’s security requirements.

Security checklist

Use this list to review and double-check your system setup and make sure you have not missed anything.

Security feature	Default
Access classes	
Access classes have been defined	n/a
Appropriate access classes are selected in user templates	n/a
Restriction/permission lists (RPLs)	
Restriction/permission lists have been defined	0 - 9 for all RPLs. This restricts <i>all</i> phone numbers.

Security feature	Default
<p>RPLs have been applied to the following features in each mailbox class:</p> <ul style="list-style-type: none"> ■ external Call Sender ■ Mailbox Thru-Dialing ■ Custom Revert ■ Delivery to Telephone/Delivery to Fax ■ AMIS Open Networking ■ Remote Notification ■ Fax Printing 	on-switch RPL
A system-wide RPL has been applied to Call Answering/Express Voice Messaging thru-dial.	on-switch RPL
An appropriate RPL has been assigned to each Application Builder service that has a thru-dial block.	on-switch RPL
An appropriate RPL has been assigned to the SDN of each Application Builder service that allows callback fax delivery.	on-switch RPL
Mailbox security	
Call Answering/Express Voice Messaging thru-dial restriction/permission list	on-switch
Password prefix	blank
Minimum password length	4
Maximum days permitted between password changes	90 days
Password expiry warning	5 days
Minimum number of changes before repeats	5

Security feature	Default
External logon	Enabled
Maximum invalid logon attempts per mailbox	9
Maximum invalid logon attempts per session	3

See also

Configure the settings listed in the checklist after system installation. Detailed information and procedures are in the following chapters in the *Administrator's Guide*:

- “Setting up restriction/permission lists”
- “Setting up mailbox security”
- “Setting up access classes for administrative users”

Restrict administrators' access to the system

Introduction

You might need to distribute the administration of the CallPilot system among several people. However, for security reasons, give administrators access to only those parts of the system they need to do their jobs.

For example, some administrators might only need to add and modify users, and others might only need to create Application Builder services.

How to restrict access to the system

Assigning appropriate access rights to different administrators involves

1. setting up access classes
2. assigning the appropriate access class to administrators

Setting up access classes

Access classes are accessed from User Administration. Access classes specify the objects to which an administrator has access. Objects are parts of the system, such as Application Builder and Mailbox classes, as well as system resources.

Access levels

In each access class, you must specify the level of access for each listed system object. For example, in one access class you might give read-only access to Application Builder. In another you might provide full access so that the administrator can create and modify applications.

See also

For more information, see “Setting up mailbox classes” in the *Administrator's Guide*.

Assigning access classes

To add an administrative user, you must do the following actions:

1. Create a user template in which administrative capabilities are enabled and the appropriate access class is selected.
2. Create the user from the template.

This means that you either have to create one user template for each type of administrator, or you have to make sure you have selected the appropriate access class in the template before you add an administrative user.

See also

For information about creating user templates, see the *Administrator's Guide*.

For information about adding users, see the *Administrator's Guide*.

Place dialing restrictions on features

Introduction

A number of CallPilot features use the switch to place calls outside your private network (on the public telephone network). This means that these features can incur long distance charges. For example, they can potentially be used to make long-distance calls. Examples of such services include Delivery to Telephone and Mailbox Thru-Dialing.

How to protect these services

To apply dialing restrictions to these features, follow a two-step process:

1. Create restriction/permission lists (RPLs).
2. Apply the appropriate restriction/permission list to services.

Create restriction/permission lists

You can define up to 200 different restriction/permission lists. This involves defining up to 30 permission codes and up to 30 restriction codes for each list. The restriction codes specify the numbers to which calls cannot be made. The permission codes specify the exceptions to the restricted codes.

Do not simply create one RPL for all services. Assign an appropriate list to each service. This might mean creating a custom RPL for each service if needed, or creating RPLs that can apply to several services that share the same requirements for dialing privileges.

Example

You need to create an RPL that restricts all long distance dialing except to the area code 514, which is where your branch office is located. You enter 91 as a restriction code (to restrict all long distance dialing), and 91514 as a permission code to allow calls to this long distance area code only.

See also

For more information, see “Setting up restriction/permission lists” in the *Administrator’s Guide*.

Apply restriction/permission lists

Once you define your restriction/permission lists, you need to apply them to services. This table summarizes the features to which you can apply restriction/permission lists:

Service	Where RPLs are applied
External Call Sender Mailbox Thru-Dialing Custom Revert Delivery to Telephone/Delivery to Fax AMIS Open Networking Remote Notification Fax Printing	User Administration, Mailbox classes, on the RPLs tab in “Setting up mailbox classes” in the <i>Administrator’s Guide</i>
Call Answering/Express Voice Messaging thru-dial	CallPilot, Security, on the General tab in “Setting up mailbox security” in the <i>Administrator’s Guide</i>
Application Builder services with thru-dial	In the application itself; see the <i>Application Builder Guide</i>
with callback fax delivery	In the SDN Table, Session profile tab in “Assigning SDNs to services” in the <i>Administrator’s Guide</i>

Secure users' mailboxes

Introduction

User mailboxes are common targets of hackers on messaging systems. CallPilot provides several ways to maximize the security of users' mailboxes.

Passwords

Use the following features to force users to create passwords that are difficult for hackers to guess. Secure passwords increase the overall security of your system:

- password prefix
- minimum password length
- maximum days permitted between password changes
- password expiry warning
- minimum number of password changes required before repeats of passwords are allowed

Invalid logon attempts

It is also important to limit the number of invalid logon attempts that can be made on a mailbox. An invalid logon attempt means that an incorrect password has been entered when trying to log on. A series of incorrect passwords is usually a sign that someone is trying to gain access to a mailbox by guessing the password. If you do not limit the number of invalid attempts, it is much easier for hackers to access mailboxes on your system.

External logon

External logon refers to the ability to log on to a mailbox from an external phone. Normally, this function is enabled (by default) so that users can call in to CallPilot and retrieve their messages when they are away from the office. However, external logon can be temporarily disabled in case of an emergency, such as a hacker attack.

See also

For information on how to configure these security features, see the *Administrator's Guide*.

Chapter 18

Monitoring and auditing CallPilot system activity

In this chapter

Overview	442
Section A: Reporter alerts and reports	445
What are alerts and reports?	446
Security alerts	448
Reports	451
Section B: CallPilot server tools	455
Alarms and events	456
Server Performance Monitor	457
Windows NT Performance Monitor	458

Overview

Introduction

This chapter describes the tools and methods available for monitoring your system's security. Once you have installed CallPilot and implemented a security policy, regularly monitor your system for unusual activity that might indicate a security problem.

Hackers can gain access to many secured systems because these systems are not properly or regularly monitored. This chapter describes the tools available to monitor traffic patterns, usage patterns, and system performance, all of which can be valuable indicators of security problems.

Establish a baseline

To recognize unusual system behavior, you need to establish a baseline. A baseline is simply a pattern that represents what is normal for your system. The only way to recognize something unusual is to know what is normal. Start using the tools described in this chapter as soon as your system is installed to get to know the normal usage patterns and performance levels for your system.

Look for unusual patterns

Once you have established a baseline, monitor your system regularly so that you can recognize potential security problems as soon as possible. You might be able to catch a problem before much damage is done.

Available tools

There are four ways to monitor your system:

- Use Reporter to generate and analyze reports on traffic patterns and feature usage that can alert you to possible security problems.
- Use CallPilot server tools to look for suspicious events and to monitor server performance levels.
- Use Windows NT Server tools.

- Use Hacker Monitoring if you suspect hackers have gained access or are trying to gain access to your system.

Use Reporter to monitor your system

The CallPilot server collects operational measurements (OMs). OMs provide statistics about how the system is being used, traffic and usage patterns, and system resource usage.

- **Reports**

Reporter allows you to regularly download OMs from the server. Downloaded OMs are then used to populate reports that you have customized so that you can view the information that is important to you. Reports can also be printed according to a print schedule to make regular monitoring easier.

Use these reports to identify the normal usage and traffic patterns for your system. Continue to use Reporter to monitor and analyze data for significant differences from your normal patterns.

- **Alerts**

Alerts are triggered whenever a preset threshold is reached. There are a number of security alerts. For example, the Excessive After-Hour Logons alert can call attention to suspicious activity.

Use CallPilot server tools

You can use a number of tools on the CallPilot server as part of your regular monitoring routine:

- Event Browser and Alarms Monitor notify you of the events and alarms generated by CallPilot. Look for events that indicate security problems.
- Performance Monitor allows you to monitor server performance levels. In some cases, deterioration in performance can be the result of a system attack.

Use Windows NT Server tools

Use the Windows NT Performance Monitor to monitor other types of server activity not captured by CallPilot server tools. This tool gives more detailed information about resource usage.

For more information, see your Windows NT documentation.

Use Hacker Monitoring

If you suspect hacker activity because of events, alerts, reports, or user complaints, use Hacker Monitoring to notify of further actions in real time. You can monitor logon attempts and thru-dials from suspected calling line IDs (CLIDs) or mailboxes. You can also monitor thru-dials from Application Builder services that have thru-dial capabilities.

For more information about Hacker Monitoring, see [Chapter 19, “Using Hacker Monitoring.”](#)

Section A: Reporter alerts and reports

In this section

What are alerts and reports?	446
Security alerts	448
Reports	451

What are alerts and reports?

Alerts

Alerts warn you of potential problems with the system's hardware, software, and security. Three alerts warn you of possible hacker activity.

Alerts are not based on real time. They analyze the previous day's operational measurement (OM) data for problems with the system. Alerts are typically calculated each day and are a convenient way of checking for any conditions that require further attention.

How alerts work

You define a threshold for each alert. This threshold is the number of OMs that must be generated for an alert to be triggered. The information created by triggered alerts is displayed in alert reports.

Example

If the threshold value of the Excessive After-Hours Logons Alert is set to 25, and 26 or more after-hour logon attempts occur, the alert is triggered.

Warning signals that indicate alerts exist

If an alert is generated, you are notified in one of two ways. Whenever you notice one of these signals, check the alert report in Reporter:

- The Communicator icon flashes on and off.
- The alert appears red in the Reporter window.

Reports

You can generate reports regularly to obtain information about how your system is being used. Unlike alerts, reports are not triggered by thresholds, but are generated regularly based on the schedule you have set up.

Regular monitoring is crucial to noticing unusual patterns that may represent hacker activity. Generate and analyze the reports described in this chapter regularly to increase system security.

See also

This chapter describes the reports that are relevant to monitoring your system's security. For detailed information on setting up Reporter and interpreting reports, see the *Reporter Guide*.

Security alerts

Introduction

For security alerts, define appropriate thresholds that determine when they are triggered. If you suspect hacker activity, you can set these thresholds lower so that you are notified sooner and more often.

Excessive incomplete messaging accesses

This alert notifies you of unsuccessful logon attempts. A high number of unsuccessful logon attempts can indicate a hacker attack. Hackers trying to find mailboxes to access enter passwords until they find one that works. Many of their attempted logons will, therefore, be unsuccessful.

Note: This alert is available only with the advanced version of the Reporter program.

Actions

If this alert is triggered, do the following actions:

1. Use the Search Users tool to search for all users with a certain number of invalid logon attempts on their mailboxes. For example, find all users who have six or more invalid logon attempts logged. This gives you a list of mailboxes that may be the targets of hackers.

For more information about using the Search Users tool, see “Maintaining existing users” in the *Administrator’s Guide*.
2. Check suspicious mailboxes by generating the Mailbox Call Session Summary report to analyze mailbox activity. Also use this report to identify the DNs of callers who have been calling in to mailboxes.
3. Enable Hacker Monitoring to monitor either
 - logon attempts to and thru-dials from suspected mailboxes
 - suspected CLIDs (the caller DNs identified in the Mailbox Call Session Summary report)

Excessive after-hours logon attempts

This alert can indicate that hackers are accessing mailboxes after hours when they are less likely to be noticed. This alert lists the mailboxes that have too many after-hours logon attempts and the caller DNs from which the logon attempts originated.

Actions

If this alert is triggered, enable Hacker Monitoring to monitor either

- the mailboxes that have excessive after-hours logon attempts
- the CLIDs (caller DNs reported by the alert) you have identified as the sources of after-hour logon attempts

Excessive thru-dialer accesses

A number of CallPilot features allow thru-dialing to the public network. This alert can indicate that hackers have gained access to your system and are placing long distance calls using thru-dial capabilities.

Actions

If this alert is triggered, find out if thru-dials are being placed from within mailboxes or from Application Builder services. You can do the following actions to investigate further:

1. Generate the Building Block Summary report to see if too many thru-dials are being placed from services created with Application Builder. Make sure the report includes information about the thru-dial block.
2. Enable Hacker Monitoring to monitor
 - thru-dials from specific mailboxes (or all mailboxes if you cannot identify the mailboxes being used)
 - thru-dials from specific Application Builder services (or all services if you cannot identify particular services as suspect)

For more information, see [Chapter 19, "Using Hacker Monitoring."](#)
3. If a particular Application Builder service's thru-dialing capability is being abused, check the restriction/permission list that is assigned to the service. You might have to restrict all long distance dialing for the service.

For more information, see the *Application Builder Guide*.

Reports

Introduction

You can generate the following types of reports to obtain information about how your system is being used.

Messaging reports

Generate and analyze the following messaging reports regularly:

- **Inactive User report**

Generate this report to find inactive mailboxes. This report informs you of the number of unread messages in the mailbox and the last time the mailbox was accessed.

Actions

Follow up with users to see if these mailboxes are no longer needed. Delete mailboxes from the system if they are unused. For mailboxes that are still being used, find out why they appear to be inactive. Check whether the users need some training. A mailbox that appears to be inactive can be a target of hackers.

- **Mailbox Call Session Summary report**

If you suspect a hacker is trying to get into a particular mailbox, generate and analyze this report to see the usage pattern over a certain period of time. This report collects information about the type of call session (Call Answering, Express Voice Messaging), the session length, the date and time, and the DN of the caller who called in to the mailbox.

Actions

If the activity looks suspicious, enable Hacker Monitoring for the mailbox so that you are notified of logon attempts to and/or thru-dials from the mailbox in real time. You can also monitor mailbox logon attempts from suspicious CLIDs (called Caller DNs in this report).

- **Voice Messaging Activity report**

This report collects summary data about messaging activity on your system. It reports on the number of Call Answering and Express Voice Messaging sessions, the number of logon sessions, the average session length, and the longest session length.

- **Signs of possible hacker activity**

When analyzing this report, add the number of logon sessions and the number of Call Answering or Express Voice Messaging sessions. If the total does not equal the total number of messaging calls on your system, there is a system problem or possible hacker activity.

Actions

If you suspect hacker activity, examine the Excessive Incomplete Messaging Accesses alert.

Traffic reports

Generate the System Traffic Summary report to get an idea of the typical traffic patterns for your services. You will notice unusual traffic patterns more quickly. If you notice a potential problem in this report, follow up with more detailed reports on suspected services.

You can use this report to establish baseline traffic statistics for various services. For security purposes, focus on services that are vulnerable to unauthorized use.

- **Monitoring Call Answering**

Unusually high Call Answering activity can indicate an attack on your system to gain entry through mailboxes.

- **Application Builder services**

Services created with Application Builder that allow thru-dialing or callback fax delivery are vulnerable since they provide outdialing capabilities.

If traffic patterns change unexpectedly for a particular service, do the following actions

- Generate a Building Block Summary report to check how many times the Fax Select or Thru-Dial block was accessed.

- If there are too many thru-dial accesses, enable Hacker Monitoring to monitor thru-dials from specific Application Builder services in real time.

Multimedia reports

It is important to monitor Application Builder services that provide thru-dial and fax callback capability. The Thru-Dial block allows callers to enter 0 followed by another number. Fax Select blocks that allow callback delivery allow callers to specify a fax number to which faxes should be delivered.

- **Building Block Summary report**

This report produces data about how your multimedia applications (created with Application Builder) are used. Use the report to monitor services that allow thru-dialing and/or fax callback. Look at the number of times the Thru-Dial block and Fax Select block have been accessed.

After a service has been put into service, monitor it for normal patterns. Keep looking for unusually high numbers of accesses.

Section B: CallPilot server tools

In this section

_Alarms and events	456
_Server Performance Monitor	457
_Windows NT Performance Monitor	458

Alarms and events

Event Browser and Alarm Monitor

The Event Browser and Alarms Monitor are important tools you can use to monitor your system and identify the cause of security breaches.

Monitor alarms and events regularly. Most hackers are able to gain access to systems because the systems are not properly or regularly monitored.

Server Performance Monitor

Introduction

Performance that is deteriorating can be caused by many things, including hacker activity on your system. Some types of attacks are meant to affect a system's performance.

For example, in a denial-of-service attack, a system is bombarded with traffic on a certain port or group of ports so that the services using those ports cannot respond to users' requests. Significant drops in performance can indicate this kind of attack.

Investigating service deterioration

If you notice deteriorations in performance, look at the Server Performance Monitor on the CallPilot Administration Client to see if you can identify the area of the system responsible for the problem. Is it CPU, disk, or memory usage?

See also

For more information about using the Server Performance Monitor, see [Chapter 9, "Viewing and filtering server events."](#)

Windows NT Performance Monitor

Introduction

The Windows NT Performance Monitor provides detailed server information and can be used to identify certain security-related problems.

For example, if you notice that the Remote Procedure Call (RPC) processes (Rpcss.exe) use 90 percent or more of your CPU time consistently, you can suspect a denial-of-service attack.

Consult your Windows NT documentation for details.

Chapter 19

Using Hacker Monitoring

In this chapter

Overview	460
Section A: About Hacker Monitoring	461
Overview	462
Calling line ID monitoring	464
Mailbox monitoring	466
Application Builder services monitoring	468
Section B: Setting up Hacker Monitoring	471
Opening Security Administration	472
Monitoring CLIDs for logon attempts and thru-dials	473
Removing a CLID from the monitoring list	474
Monitoring mailboxes for logon attempts and thru-dials	475
Removing a mailbox from the monitoring list	476
Monitoring Application Builder applications for thru-dials	477
Removing an Application Builder application from the monitoring list	478
Setting up an alarm mailbox	479
Viewing alarms	481

Overview

Introduction

If you have noticed suspicious activity on your system, enable and set up Hacker Monitoring to track and notify you of suspicious activity in real-time. This chapter describes how to set up Hacker Monitoring to track different types of activity and how to make sure you receive notification of specific events immediately.

Section A: About Hacker Monitoring

In this section

Overview	462
Calling line ID monitoring	464
Mailbox monitoring	466
Application Builder services monitoring	468

Overview

Introduction

Hacker Monitoring is a feature that, using a combination of CallPilot tools, allows you to monitor CallPilot for certain events that you suspect are caused by hackers who have gained access to your system. When the event you are monitoring occurs, an alarm is generated. This means you are notified of suspicious activity in real time so you can investigate immediately.

When to use Hacker Monitoring

Generally, you use Hacker Monitoring only when you suspect hacker activity on your system. You are alerted to this activity in several ways.

- Users complain of suspicious behavior in their mailboxes, such as changed greetings or obscene messages.
- An alert is triggered by Reporter.
- A report generated in Reporter indicates unusual traffic or usage patterns.

What you can monitor

What you monitor depends on the type of suspicious behavior you have noticed. You can use Hacker Monitoring to monitor

- internal and external telephone numbers (CLIDs) from which you suspect hackers are calling
- mailboxes to which you suspect hackers have gained access
- Application Builder services you suspect hackers are using to place thru-dials

Receiving notification of alarms

If, for example, you enable Hacker Monitoring for a particular mailbox, all logon attempts to that mailbox cause an alarm to be generated. You can find out about the alarms generated by Hacker Monitoring by

- viewing the Alarms Monitor regularly to learn of new alarms
- setting up an alarm mailbox so that whenever an alarm is generated, the system sends a voice message to the mailbox to alert you
- enabling Remote Notification for the alarm mailbox so you are notified of new alarm messages immediately at a specified number, such as a pager or cell phone

Calling line ID monitoring

Introduction

When a call comes in to the system, CallPilot keeps track of the calling line ID (CLID), if available. The CLID identifies a caller to the system. If you have identified certain CLIDs as suspicious (possibly the number from which a hacker is calling in to your system), you can monitor them with Hacker Monitoring.

How to identify suspicious CLIDs

You might become suspicious of certain CLIDs under the following conditions:

- You receive an Excessive After-Hours Logons alert. This alert reports the mailbox number and caller DN (the CLID).
- You run the Mailbox Call Session Summary report on mailboxes you suspect are targets of hackers and notice calls repeatedly originating from certain caller DNs.

Logon attempts and thru-dials

For CLIDs, you can monitor thru-dials or logon attempts, or both.

When thru-dials are monitored, an alarm is generated whenever a monitored CLID gains access to the system and places a thru-dial. It does not matter how the caller thru-dialed—whether it was from a mailbox or an Application Builder service, for example. All thru-dials originated from the monitored CLID generate an alarm.

Internal and external CLIDs

You can monitor both internal CLIDs (extensions) and external CLIDs. You might suspect that certain users are using features in an unauthorized way and decide to track specific internal numbers. Monitor external CLIDs when you suspect hackers are accessing your system from the outside.

Generated alarms

The following alarms are generated whenever a logon or thru-dial originates from a monitored CLID:

Event number	Description
55750	Successful login from Hacker Monitored DN.
55751	Failed login from Hacker Monitored DN.
55752	Thru-dial in mailbox from Hacker Monitored DN.
55753	Thru-dial attempt in mailbox from Hacker Monitored DN.
55754	Thru-dial in Application Builder application from Hacker Monitored DN.
55755	Thru-dial attempt in Application Builder application from Hacker Monitored DN.

Actions

If a specific mailbox is being targeted, find out if the mailbox is in use. If it is being used, inform the user and ask him or her to change the mailbox password immediately.

If the mailbox is unused, delete it immediately.

Mailbox monitoring

Introduction

If you suspect that hackers are trying to gain access or have gained access to certain mailboxes, enable Hacker Monitoring to monitor specific mailboxes.

If you suspect a major attack on your system, you might need to monitor all mailboxes for some time until you can deal with the problem.

Thru-dials and logon attempts

You can monitor mailboxes for all logon attempts or thru-dials, or both.

If you suspect that hackers have set up mailboxes on the system and are using them for their own purposes, monitor logons.

If you suspect that hackers are using mailboxes to access thru-dial capabilities, monitor the thru-dials made from suspect mailboxes.

Generated alarms

The following alarms are generated whenever there is a logon to or a thru-dial from a monitored mailbox:

Event number	Description
55756	Failed login attempt to Hacker Monitored mailbox.
55757	Failed login attempt to Hacker Monitored mailbox.
55758	Successful login to Hacker Monitored mailbox.
55759	Successful login to Hacker Monitored mailbox.
55760	Successful thru-dial from Hacker Monitored mailbox.
55761	Successful thru-dial from Hacker Monitored mailbox.

Event number	Description
55762	Thru-dial attempt from Hacker Monitored mailbox.
55763	Thru-dial attempt from Hacker Monitored mailbox.

Actions

If Hacker Monitoring reveals that a mailbox has been compromised, follow up to identify its status.

Access the user's profile from User Administration. On the Security tab, check the time of the last logon and when the password was last changed. If the mailbox has not been accessed for a while, the mailbox might no longer be used. Contact the user or find out if the user has left your organization.

IF	THEN
the user has left your organization and the mailbox is no longer needed	delete the mailbox immediately.
the user is on vacation or absent for a long time	you need to decide whether to <ul style="list-style-type: none"> ■ disable the mailbox until the user gets back. ■ change the password.
the user is present and the mailbox is needed	ask the user if he or she has noticed any strange behavior. The user might need training on how to use the mailbox. Ask the user to change the password to a secure password immediately.

Application Builder services monitoring

Introduction

Application Builder services can become targets of hackers if they include a Thru-Dial block that allows callers to make calls to the public switched telephone network (PSTN).

Building Block Summary report

You will most likely be alerted to security problems in Application Builder services by running and analyzing the Building Block Summary report. Look at Thru-Dial block accesses to see if there is an unusually high number.

To follow up, enable Hacker Monitoring to monitor selected Application Builder services or all Application Builder services. Any time there is a thru-dial from the monitored service, an alarm is generated.

Generated alarms

The following alarms are generated whenever a thru-dial is originated from a monitored Application Builder service:

Event number	Description
55764	Thru-dial from Hacker Monitored Application Builder application DN.
55765	Thru-dial from Hacker Monitored Application Builder application DN.
55766	Thru-dial attempt from Hacker Monitored Application Builder application DN.
55767	Thru-dial attempt from Hacker Monitored Application Builder application DN.

Actions

If Hacker Monitoring confirms that a certain service is being used to thru-dial in an unauthorized way, check the design of your service.

Restriction/permission lists

Check the restriction/permission list that has been assigned to the service. Can you assign a more restrictive list without a significant impact on users of the service?

Password blocks

Use password blocks if possible. For example, if you want only some users to be able to place long distance thru-dials, you can create two Thru-Dial blocks and assign a different restriction/permission list to each one. In front of the Thru-Dial block that allows long distance dialing, insert a Password Check block that requires users to enter a password before accessing that part of the service.

See also

For more information on blocks in Application Builder, see the *Application Builder Guide*.

Section B: Setting up Hacker Monitoring

In this section

<u>Opening Security Administration</u>	<u>472</u>
<u>Monitoring CLIDs for logon attempts and thru-dials</u>	<u>473</u>
<u>Removing a CLID from the monitoring list</u>	<u>474</u>
<u>Monitoring mailboxes for logon attempts and thru-dials</u>	<u>475</u>
<u>Removing a mailbox from the monitoring list</u>	<u>476</u>
<u>Monitoring Application Builder applications for thru-dials</u>	<u>477</u>
<u>Removing an Application Builder application from the monitoring list</u>	<u>478</u>
<u>Setting up an alarm mailbox</u>	<u>479</u>
<u>Viewing alarms</u>	<u>481</u>

Opening Security Administration

Introduction

To perform the procedures in this section, you must open the Security Administration program.

Getting there CallPilot System > Messaging Administration > Security Administration

To access Security Administration

- 1 Double-click Security Administration.



Result: The Security Administration Properties window appears.

Monitoring CLIDs for logon attempts and thru-dials

Introduction

Monitor specified calling line IDs (CLIDs) either on or outside your system to track suspicious thru-dial activities and logon attempts. Every time a logon or a thru-dial is made by the monitored CLID, an event code is generated.

Getting there CallPilot System > Messaging Administration > Security Administration > CLIDs tab

To monitor CLIDs for suspicious behavior

- 1 To monitor CLIDs, make sure the Monitor CLIDs for all mailbox logon attempts and thru-dials on the system check box is checked.
- 2 To set up a monitoring period for CLIDs, in the Monitoring period from list, type or select the time to start monitoring in hours and minutes in a 24-hour format.
- 3 In the Monitoring period to list, type or select the time to stop monitoring in hours and minutes in a 24-hour format.
- 4 To monitor a CLID that is on the local switch, type the DN in the Internal box.
- 5 Click Add to include the CLID in the list of internal CLIDs.
- 6 To monitor a CLID that is external to the switch, type the DN in the External box.
- 7 Click Add to include the CLID in the list of external CLIDs.
- 8 Click Save.

Removing a CLID from the monitoring list

Introduction

Remove a CLID from the list of CLIDs that the system is monitoring when you have determined the cause of suspicious activity and have resolved the problem.

Getting there CallPilot System > Messaging Administration > Security Administration > CLIDs tab

To remove a CLID from monitoring

- 1 In the Internal CLIDs list, select the CLID you want to remove.
- 2 Click Delete.
- 3 In the External CLIDs list, select the CLID you want to remove.
- 4 Click Delete.
- 5 Click Save.

Monitoring mailboxes for logon attempts and thru-dials

Introduction

Monitor specific mailboxes on your system to track suspicious thru-dial activities and logon attempts. Every time someone logs on to a mailbox or places a thru-dial call from it, an event code is generated.

Getting there CallPilot System > Messaging Administration > Security Administration > Mailboxes tab

To monitor mailboxes for suspicious behavior

- 1 To monitor logon attempts to specified mailboxes, make sure the Logins check box is checked.
- 2 To monitor thru-dials made from specified mailboxes (during either Messaging or Call Answering sessions), make sure the Thru-dials check box is checked.
- 3 To set the monitoring period, in the Monitoring period from list, type or select the start time in 24-hour format.
- 4 To end the monitoring period, in the Monitoring period to list, type or select the end time in 24-hour format.
- 5 To monitor every mailbox on the system, make sure the All check box is checked.
- 6 To monitor only the mailboxes that you include in the list, make sure the Selected check box is checked.
- 7 If you enabled Selected to include a mailbox, type the mailbox number in the mailbox DN box (the unmarked box on the left).
- 8 Click Add.
- 9 Repeat steps [7](#) to [8](#) for each additional mailbox you want to monitor.
- 10 Click Save.

Removing a mailbox from the monitoring list

Introduction

Remove a mailbox DN from the monitoring list when you have determined the cause of suspicious activity and have resolved the problem.

Getting there CallPilot System > Messaging Administration > Security Administration > Mailboxes tab

To remove a mailbox from monitoring

- 1 In the list of mailbox DN's, select the mailbox you want to stop monitoring.
- 2 Click Delete.
- 3 Click Save.

Monitoring Application Builder applications for thru-dials

Introduction

Monitor specified Application Builder applications to track suspicious thru-dial activities. Every time a thru-dial is made from the application (specified by its SDN), an event code is generated.

Getting there CallPilot System > Messaging Administration > Security Administration > AppBuilder tab

To monitor Application Builder services for suspicious behavior

- 1 To monitor thru-dials made from specific Application Builder applications, make sure the Monitor thru-dials for AppBuilder entries in the SDN table check box is checked.
- 2 To set the monitoring period, in the Monitoring period from list, type or select the start time in 24-hour format.
- 3 To end the monitoring period, in the Monitoring period to list, type or select the end time in 24-hour format.
- 4 To monitor every Application Builder application in the SDN Table, make sure the All check box is checked.
- 5 To monitor only specific applications, make sure the Selected check box is checked.
- 6 If you enabled Selected to include an SDN, type the DN associated with the Application Builder application in the Application DN box (the unmarked box on the left).
- 7 Click Add.
- 8 Click Save.

Removing an Application Builder application from the monitoring list

Introduction

Remove an application's SDN from the monitoring list when you have determined the cause of suspicious activity and have resolved the problem.

Getting there CallPilot System > Messaging Administration > Security Administration > AppBuilder tab

To remove an Application Builder application from monitoring

- 1 In the list of monitored application DNs, select the SDN you want to remove.
- 2 Click Delete.
- 3 Click Save.

Setting up an alarm mailbox

Introduction

Define an alarm mailbox if you want CallPilot to send you (or another administrator) a voice message when an alarm is generated. The message notifies you that an alarm has been received. The message is tagged as urgent. After receiving a notification message, look at the Alarms Monitor to get more details.

Immediate notification of alarm messages

If you want to be notified immediately of new alarms generated by Hacker Monitoring, enable Remote Notification (RN) for the alarm mailbox. If you are away from the phone and cannot see that the Message Waiting Indicator (MWI) has been turned on, the RN service sends a message at the number you have defined. This can be a pager or another phone, such as a cell phone.

Note: Remote Notification must be enabled in the mailbox class to which the alarm mailbox is assigned.

Getting there CallPilot System > Messaging Administration > Messaging Administration

To set up an alarm mailbox

- 1 Double-click Messaging Administration.
- 2 Click the Mailboxes tab.
- 3 In the Alarm mailbox number box, enter the number of the mailbox to which you want alarm notification messages to be sent.

Note: If you want remote notification of alarm messages, make sure this mailbox belongs to a mailbox class in which RN is enabled.

- 4 In the Severity to trigger box, specify whether you want critical, major, or minor alarms to cause a message to be sent to the alarm mailbox.

Note: To disable the alarm mailbox, select none.

- 5 Click Save.

To enable Remote Notification for the alarm mailbox

- 1 Make sure the alarm mailbox is assigned to a mailbox class in which Remote Notification is enabled.
- 2 Create a notification schedule.

For more information on verifying or changing the mailbox class assignment, as well as information on setting up a remote notification schedule, see [Chapter 4, “Maintaining existing users.”](#)

Viewing alarms

Introduction

To obtain information about an alarm generated within the system, use the Event Browser and Alarm Monitor.

Event Browser

The Event Browser lets you view events that have been recorded in the server log. Use the Event Browser to view the time an event occurred, the object that generated the event, and the cause of the event.

To reduce the number of events shown in the Event Browser at one time, you can set up a filter that screens the log for events that meet your specifications. Events can be filtered according to their code, type, severity, or interval.

For instructions on using the Event Browser, see [Section A: “Using the Event Browser,” on page 271](#).

Alarm Monitor

Once an alarm has been raised, it is displayed in the Alarm Monitor window. From this window, you can view the details of an alarm, such as the code and severity of the event that raised the alarm, the time at which the event was logged, the program that generated the event, and the cause of the event.

For instructions on using the Alarm Monitor, see [Section B: “Using the Alarm Monitor,” on page 281](#).

Chapter 20

Security features on the Meridian 1 switch

In this chapter

Overview	484
Understanding dialing restrictions	487
Network Class of Service	490
Trunk Group Access Restriction and Class of Service	494
Coordinating Meridian 1 and CallPilot dialing privileges	498
Meridian Mail Trunk Access Restriction	500
Precautions for modems	501

Overview

Introduction

This chapter describes Meridian 1 switch features that affect the security of your CallPilot system. These features interact with features in CallPilot, and should be considered when designing and implementing a security policy.

Note: This chapter describes features on the Meridian 1 switch only. If your system is connected to a different switch, refer to your switch documentation for security features.

A number of CallPilot services can call out of your private Meridian 1 switch and onto the public switched telephone network (PSTN). These include

- Thru-dialing from mailboxes, Call Answering sessions, and Express Voice Messaging sessions
- External Call Sender
- user-defined revert DN's (Custom Revert)
- outcalling services (Delivery to Telephone, Delivery to Fax, Remote Notification)
- services created with Application Builder that allow users to enter a fax callback number
- AMIS Open Networking

Implications

These services are susceptible to toll fraud. Take the necessary precautions to ensure that they are not abused. The calls these features place originate from your Meridian 1 and are, therefore, charged to your company.

Restriction/permission lists (RPLs)

In CallPilot, you can create up to 200 restriction/permission lists (RPLs). You can then assign a list to each CallPilot service that can make outgoing calls. RPLs determine the numbers that CallPilot services can and cannot call.

By default on a newly installed system, all codes (from 0 to 9) are defined as restriction codes in all lists. This means that all of the listed services are completely restricted from placing calls and will not work until you modify the RPLs. This forces you to consider the numbers you want to allow and deny for each service.

Example

Generally, you want to prevent Delivery to Telephone from placing international calls. However, you have branch offices in Paris and Osaka to which users send messages. In the RPL for Delivery to Telephone, you enter the international network access code (9011, for example) as a restriction code to block international dialing. However, you enter 9011331 and 9011816 as permission codes to allow calls to Paris and Osaka.

Multiple layers of defense

RPLs are a good first line of defense. However, they should not be your only defence. Errors in RPL setup or oversights can lead to a security hole. Use the features on the Meridian 1 together with RPLs to create multiple security checkpoints.

Restrictions you can place on agents

CallPilot uses ACD agents on the Meridian 1 to accept incoming calls and to place outgoing calls. Whereas RPLs are applied to specific CallPilot services, on the Meridian 1, restrictions are placed on agents to control access rights to trunks and dialing privileges.

The following Meridian 1 features should be used in addition to restriction/permission lists. CallPilot agents are configured as digital sets (type 2008) in Overlay 11:

- Trunk Group Access Restrictions (TGARs/TARGs)
- Class of Service (CLS)
- Network Class of Service (NCOS)

See also

See your Meridian 1 documentation for detailed information about switch security. There are many features that you can use to greatly increase the level of security.

This information can be found in the Meridian 1 switch *System Security Guide*.

Understanding dialing restrictions

Dialing privileges for ACD agents

CallPilot services that can place outgoing calls use ACD agents on the Meridian 1 to do so. The dialing privileges given to these agents must allow CallPilot services to dial out to the required numbers (local and long distance). However, do not make dialing privileges more permissive than they need to be. When assigning dialing privileges, balance security and convenience.

Features that restrict outbound calls

Some features in CallPilot and on the Meridian 1 can be used together to provide CallPilot agents with the appropriate dialing privileges. Use these features together to layer security checkpoints, rather than relying on just one feature.

Feature	Description
In CallPilot	
Restriction/permission lists (RPLs)	<p>RPLs are your first line of defense. You must assign an RPL to each service that can outdial. The RPL identifies which dialing codes are restricted and which are allowed.</p> <p>For more information, see “Setting up restriction/permission lists” in the <i>Administrator’s Guide</i>.</p>
On the Meridian 1	
Network Class of Service (NCOS)	<p>NCOS is a BARS/NARS feature that determines the numbers that can and cannot be called by CallPilot agents.</p>
Trunk Group Access Restrictions (TGARs)	<p>TGAR controls which direct access trunks CallPilot agents can use. Nortel Networks recommend that agents not be allowed direct access to trunks.</p>
Class of Service (CLS)	<p>CLS controls dialing privileges (local calls only, long distance, and so on) on the direct access trunks that CallPilot agents are allowed to use.</p>

What determines whether a call is allowed

When a CallPilot service tries to place an outgoing call to a certain telephone number, several factors determine whether the call is allowed. Here is what happens:

1. A CallPilot service tries to place an outbound call.

Example: A user tries to thru-dial to an international number (901133142950247) from a mailbox.

2. The system checks the assigned restriction/permission list (RPL).

Example: The system checks the user's mailbox class to see if the RPL assigned to the Mailbox Thru-Dial feature allows calls to the dialed number.

- If any of the starting digits in the dialed number are restricted (such as 9011), then the call is blocked.
 - If the starting digits are not defined as a restricted code or are defined as a permitted code, then the Meridian 1 switch settings are checked.
3. The NCOS assigned to the agent is checked to see if the dialed number is restricted.
 - If the number is restricted, the call is blocked.
 - If the number is not restricted, and Trunk Group Access Restrictions (TGAR) is also implemented, the TGAR setting is checked. (If TGAR is not implemented, the call is made at this point.)
 4. The TGAR assigned to the agent is checked and compared to the Trunk Access Restriction Groups (TARGs) assigned to the trunk route the service is trying to use.
 - If the TGAR matches one of the TARGs, then the call is blocked.
 - If there is no match, then the Class of Service (CLS) is checked.
 5. The CLS assigned to the agent is checked to determine the calling privileges. If the CLS allows international calls, then the call is placed.

Implications

In CallPilot, restrictions are assigned on a feature-by-feature basis. For example, you can assign one RPL (that allows on-switch and local calls) to Delivery to Telephone and another RPL (that allows on-switch calls only) to Call Answering/Express Voice Messaging thru-dial.

On the Meridian 1, however, restrictions are assigned per agent. Since all ACD agents that service CallPilot are put into one ACD queue, you cannot control which agent is used by which service. Therefore, restrictions assigned to agents must allow CallPilot services to place calls to the numbers required by your business.

However, agents should not be left completely unrestricted. If an RPL is not set up properly, or the incorrect RPL is assigned to a feature, the restrictions placed on agents can be a secondary defense that blocks calls from getting through to destinations that should be restricted.

Network Class of Service

Introduction

When a user or a CallPilot service dials a number that begins with a network access code (such as 9 to dial out and place a local call) followed by the desired number, the BARS/NARS software processes and routes the call. Based on the dialed number, the Meridian 1 reads a digit translation table. The translation determines which list of alternate routes the system uses to process the call. This list is called a route list index and contains alternate outgoing routes (trunk groups) for call completion.

Definition

Network Class of Service (NCOS) is a BARS/NARS feature. An NCOS designation is a group of calling privileges you can assign to a station, TIE trunk, DISA DN, or authorization code. In CallPilot, you assign the ACD agents that service CallPilot to an NCOS that determines the appropriate privileges. Nortel Networks recommends that a special NCOS be set up for CallPilot agents.

Facility Restriction Levels

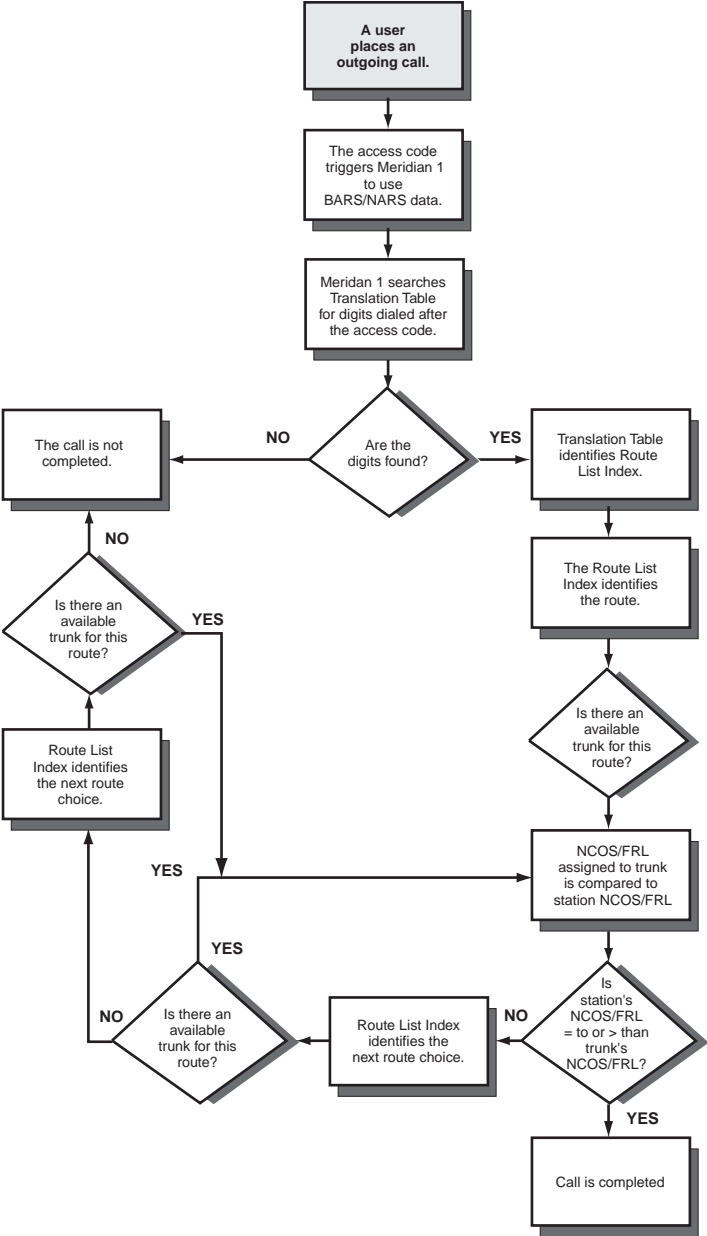
When you set up an NCOS group, you assign it a Facility Restriction Level (FRL). There are eight FRLs (0 to 7). When a service tries to place an outgoing call, the FRL of the agent's NCOS is compared to the minimum FRL requirement assigned to each entry in a route list.

The entries in the route list are trunk routes that can place calls to certain country codes, area codes, or special numbers. The routes are listed in the order the system searches them when trying to complete an external call. Agents are allowed to complete a call on an entry in the route list when their FRL is equal to, or higher than, the entry's FRL level.

Example

1. A user dials 9-1-417-555-9090.
2. The 9 triggers Meridian 1 to use BARS/NARS data.
3. The Meridian 1 searches the translation table for 1417.
Calls to 1417 use Route List Index 2.
4. Route List Index 2 is searched for an idle available trunk.
The first choice is a WATS route.
5. The NCOS/FRL assigned to the first choice (2) is compared to the NCOS/FRL (2) of the station.
The station's NCOS/FRL (2) is equal to or greater than the WATS NCOS/FRL (2), so the call is allowed for this choice.
6. If all WATS trunks are busy, then the second choice (CO trunks) is checked.
7. The NCOS/FRL of the CO trunks (3) is compared to the NCOS/FRL of the station (2).
The station's NCOS/FRL (2) is lower than the CO trunks' NCOS/FRL (3), so the call cannot be completed over CO trunks.

See the following illustration.



What about TGARs?

The BARS/NARS database can be configured to ignore Trunk Group Access Restrictions or to use them. When TGARs are ignored, the BARS/NARS software assesses the Class of Service and the FRL to determine which call facilities are eligible for a particular call. This configuration allows flexibility in using a given trunk group while forcing users to place calls through BARS/NARS. You can base trunk access for each call on the FRL requirements for the number dialed rather than basing access on the TGAR.

You can also configure the BARS/NARS database to assess TGAR assignments in determining how the system can route a call. In this case, the BARS/NARS software uses the CLS, TGAR, and FRL to determine which call facilities are eligible to process a particular call.

In either case, the most restrictive setting is used to determine whether a call can be completed.

Recommendations

Here are some recommendations and considerations for setting up NCOS for your CallPilot agents:

1. Put all CallPilot agents into one NCOS group. That way, if you need to make a change, you modify only one NCOS group.
2. When selecting an FRL for the NCOS, keep the following aspects in mind:
 - The FRL must allow CallPilot services to place calls to the necessary numbers.
 - However, the FRL should not be more permissive than necessary.
3. Since most long distance fraud calls are destined for certain specific country codes and area codes, consider not defining these codes in your translation tables if your business does not require that users call these locations. If your business requires calls to destinations associated with toll fraud, consider assigning unique route list indexes to each of these destinations. This scheme provides the capability to assess normal call volumes and to detect variations.

Trunk Group Access Restriction and Class of Service

Trunk Group Access Restriction

Trunk Group Access Restriction (TGAR) is used to allow or deny stations, or CallPilot agents in our case, the ability to dial trunks directly. Direct trunk access means that a network access code, such as 9 to dial out for local calls, is not needed. Instead, a special direct access code is needed.

Nortel Networks recommends that CallPilot agents not be able to access trunks directly.

How TGAR works

Each trunk route is configured with a list of Trunk Access Restriction Groups (TARGs) ranging from 0 to 31.

Each CallPilot agent is assigned a Trunk Group Access Restriction (TGAR). When a CallPilot service attempts to access a trunk route using an agent, the Meridian 1 compares the agent's TGAR assignment against the list of denied Trunk Access Restrictions Groups (TARGs) associated with the trunk route the service is trying to access.

TARGs and TGARs provide a way to assign values to trunk routes and agents so that they can be compared when trunk access is requested. When the agent's TGAR matches a TARG, the call is denied. If there is no match, the Class of Service (CLS) assigned to the agent is checked.

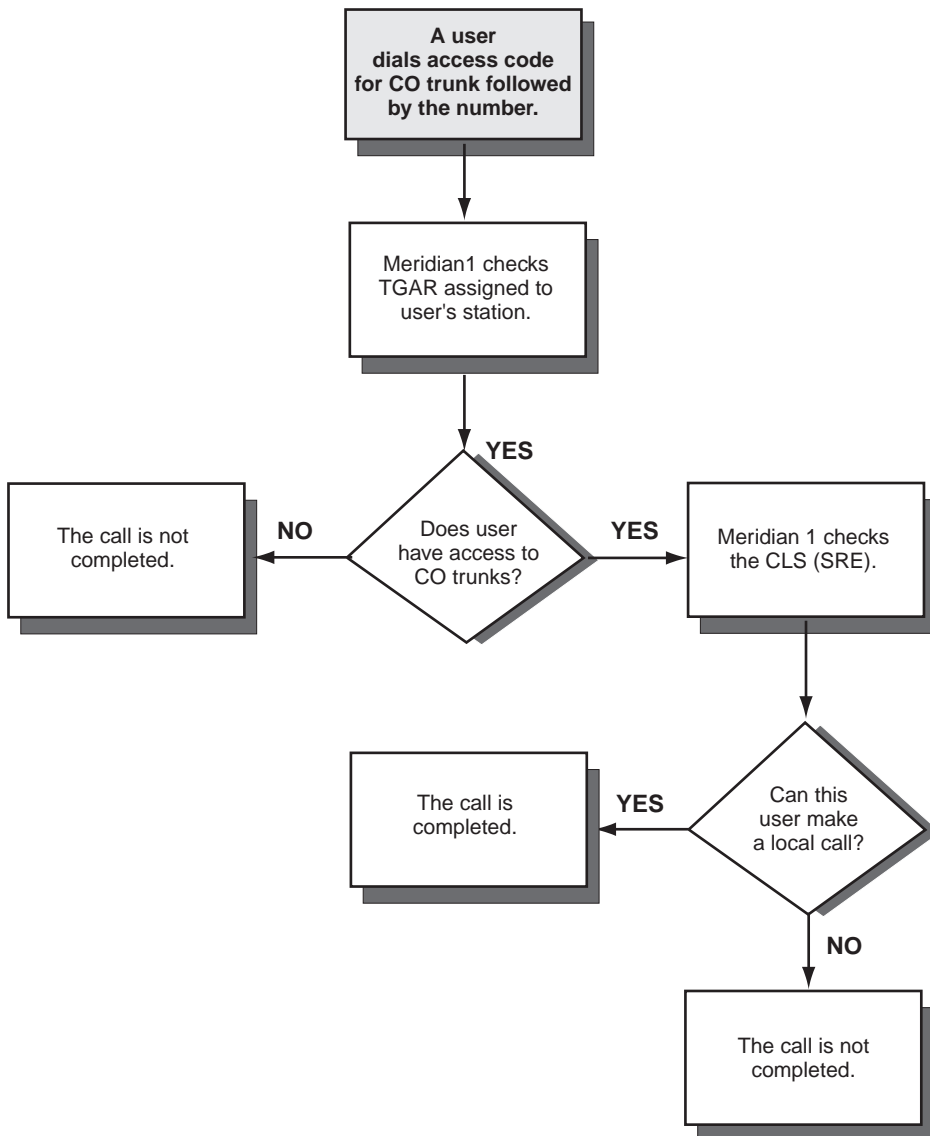
Class of Service

If the agent's TGAR permits access to the trunk route, the Meridian 1 then checks the agent's CLS assignment to determine call eligibility. The system always uses the most restrictive assignment (CLS or TGAR) to determine call eligibility when a service is trying to access trunk facilities directly. For example, if the agent's TGAR allows access to long distance trunk routes, but the CLS does not, the CLS setting is used and long distance calls are blocked.

There are many different CLS options, ranging from Unrestricted Service (UNR) to Fully Restricted Service (such as FRE and FR1).

How TGAR and CLS work together

The following illustration shows the interaction between the CLS assignment and TGARs.



In this illustration, the following events occur:

- A user dials the access code for the CO trunk group, followed by 555-6100.
- The Meridian 1 checks the TARG assigned to the user's station to see if the user has access to CO trunks. The user does.
- The Meridian 1 checks the CLS (SRE) to see if the user can make a local call. The user cannot make a local call.

Recommendations

When you assign a CLS to CallPilot agents, consider the following aspects:

- Conditionally Toll Denied (CTD) is the default class and is recommended for most systems.

CTD allows agents to receive calls from the exchange network. Agents are restricted from placing toll calls through direct access trunks, but are unrestricted for toll calls placed through Basic/Network Alternate Route Selection (BARS/NARS). This CLS forces agents' calls over BARS/NARS translations, allowing control over dialing privileges using NCOS.
- Unrestricted Service (UNR) is not recommended.

Any oversights in your restriction/permission list settings and assignments, or any modifications to these lists that run counter to your security policy, create a security hole. Outbound calls that should not get through might end up getting through with UNR.
- If you want to make sure that no CallPilot service is able to place long distance calls, you can choose a more restrictive Class of Service.

Coordinating Meridian 1 and CallPilot dialing privileges

All agents must have the same privileges

All CallPilot agents are placed in one ACD queue and cannot be dedicated to particular services. This means that there is no way of knowing which agent is used by a particular service. Therefore, all ACD agents that are used by CallPilot must have the same dialing privileges.

Implications

This means you must identify which service needs the most permissive dialing privileges and then configure all CallPilot agents with the required privileges. You do your fine-tuning in CallPilot using restriction/permission lists. Since you can create up to 200 of these lists, you can assign a different list to each service based on the dialing privileges needed by that service.

Example

Your policy is that no CallPilot services are allowed to place international calls. However, long distance dialing in the same country code is required by certain services.

This means that all agents used by CallPilot must be allowed to make long distance calls (in the same country code), but that they should all be blocked from making international calls.

In CallPilot, you assign more limited RPLs to services you do not want to allow to make long distance calls (or even local off-switch calls).

Summary of steps to take

Do the following actions to make sure dialing restrictions in CallPilot and on the Meridian 1 work together to provide the needed level of dialing privileges:

1. Determine the dialing privileges required for each of the following CallPilot services:
 - Call Answering/Express Voice Messaging thru-dial
 - services created with Application Builder that include a thru-dial and/or fax callback block

Note that, for the following services, the RPL is assigned in mailbox classes. This means you can assign a different RPL to the same feature in different mailbox classes (based on user requirements):

- Mailbox Thru-Dial
 - External Call Sender
 - Custom Revert
 - Delivery to Telephone/Delivery to Fax
 - Remote Notification
 - AMIS Open Networking
 - Fax Printing
2. Identify which services need the most permissive dialing privileges.

Example: Several of your services need to be able to place long distance calls in the same country code. International dialing is not needed by any service.
 3. Set the dialing privileges (NCOS, TGAR, CLS) for all CallPilot agents to the most permissive setting required (as identified in step 2). Do not make privileges more permissive than is necessary. Create enough restriction/permission lists to cover all the dialing privileges your services require.
 4. Create restriction/permission lists in CallPilot.

Note: Do not simply create one restriction/permission list and then assign it to all services. This can open your system to attacks. If each service requires different dialing privileges, it is better to create multiple lists and customize them for each service. Most likely, certain services share the same dialing privileges, so you can assign the same restriction/permission list to several services.

5. Assign the appropriate restriction/permission list to each service.

Meridian Mail Trunk Access Restriction

What is Meridian Mail Trunk Access Restriction?

Meridian Mail Trunk Access Restriction (MTAR) is a Meridian 1 feature that restricts the ability of a person on an internal extension from transferring or conferencing external callers within the switch.

External calls are defined as incoming/outgoing trunk calls that originate or terminate outside a private network. This definition applies to all types of trunks, except TIE trunk calls.

Why use MTAR?

MTAR prevents system abuse by distinguishing between internal and external calls directed to CallPilot. MTAR prevents completion of any Call Transfer, Conference, No Hold Conference, or Call Join attempts on incoming/outgoing external calls to CallPilot.

Example

If Anna calls David from a trunk that has an MTAR restriction, David cannot transfer the call to CallPilot. Similarly, David cannot conference Anna to CallPilot.

Precautions for modems

Introduction

CallPilot uses a modem to give technical support and service personnel remote access to the system. Modems are a common target of hackers and must be secured.

Hackers use “smart” modems to get into PBXs. Hackers take advantage of systems whose 2500 dataports are programmed with unnecessary features.

What you can do

Identify modem phones and remove the transfer feature if possible. The default on 2500 sets is “deny.” Whenever possible, ensure the CLS, TGAR, and NCOS do not allow long distance calling.

The modem port usually has calling privileges assigned that are not needed for the modem to function. Often, a 2500-set template is used that is also used for single-line phones. The administrator might be unaware that the 2500 port is used for data.

Index

A

- access classes
 - assigning 436
 - changing 83
 - setting up 435
- access, viewing last mailbox 101
- accessing
 - Backup Administrative Tool 31
 - Disk Administrator 31
 - Event Browser 273, 311
 - Event Viewer 31
 - Server Performance Monitor 31
 - User Manager 31
 - User Profile Editor 31
 - Windows NT diagnostic tools 31
- activity, tracking suspicious 413
- adding a system to the administrative PC 51
- addresses, number of, in an SDL 113
- administration, basic user maintenance 60
- administrative capability
 - adding to a user 83
 - changing for a user 84
 - removing from user 84
- administrator
 - accounts, securing 410
 - changing an access class 83
 - locking out the desktop 85
 - resetting a password 89
 - restoring access 87
 - restricting access 435
- Administrator account, changing the password
 - for 425
- after-hours mailbox access 449
 - what to do 449
- agents
 - CLS recommendations 497
 - dialing privileges 498
 - implementing 498–499
 - implications 498
 - NCOS recommendations 493
 - restrictions, implications 489
 - security restrictions 485
 - CallPilot and Meridian 1 features 487
 - dialing privileges 487
- alarm mailbox 479
 - setting up 479
 - setting up immediate notification 479, 480
- Alarm Monitor 246, 247, 263, 264, 290, 456
 - clearing active alarms 286
 - correcting recurring alarms 284
 - in the background 285
 - position 284
 - recurring alarms 284
 - sorting events 283
 - viewing events 282
- alarm, definition 246
- alarms
 - clearing 286
 - clearing active 286
 - CLID generated 465
 - what to do 465
 - correcting recurring 284
 - mailbox generated 466
 - followup 467
 - MMFS volumes 328
 - clearing 328
 - Nortel directory disk space 326
 - notification
 - Hacker Monitoring 462
 - hardware problems 253
 - printing active 309
 - printing all 309
 - working with, Alarm Monitor 246, 247
- alerts
 - how they work 446
 - warning signals 446
 - what are they? 446
- allowing calls, description 488
- Application Builder
 - archive 216
- Application Builder services
 - monitoring with Hacker Monitoring 468
 - alarms followup 469
 - Building Block Summary report 468
 - generated alarms 468

- removing from monitoring list 478
 - setting up monitoring for 477
 - Application log 266
 - archive
 - Application Builder 216
 - definition 214
 - description 214
 - frequency 215
 - how they differ from system backups 214
 - performing an immediate archive 231
 - prompt 216, 217
 - Restore Manager 217
 - restoring user data 239
 - searching for users for a user archive 227
 - setting up a customized prompts archive 228
 - setting up a schedule for an archive 229
 - setting up a user archive 224
 - setting up an Application Builder archive 221
 - types of
 - Application Builder 216
 - prompt 216
 - user 216
 - updating a User archive 225
 - updating an AppBuilder archive 222
 - user 216
 - why restore data from archives 217
 - assigning access classes 436
 - Autologon
 - disabling 97
 - enabling 97
- ## B
- backup
 - adding devices 154
 - common error codes 164
 - creating a disk device on the CallPilot server 206
 - creating a writable shared directory 179–198
 - devices, predefined 151
 - excluded data 146
 - formulating a strategy 148
 - how they differ from archives 214
 - modifying or deleting devices 156
 - monitoring and canceling 171
 - predefined server 145
 - RAID systems 144
 - remote disk 176–178
 - required security and password 145
 - requirements 145
 - restoring from 144
 - restoring your system (by CallPilot distributor) 208
 - scheduling 160–170
 - server data 144
 - speed 147
 - tape devices 151
 - viewing devices 157
 - backup and restore
 - reconfiguring on the CallPilot server 199–205
 - Backup Devices
 - accessing the window 150
 - Backup Scheduler
 - accessing the window 163
 - Backup, accessing the Administrative Tool 31
 - baseline
 - establishing, using Reports 257, 442
 - basic administration, user maintenance 60
 - behavior, system
 - establishing a baseline using Reports 257, 442
 - billing OMs 44
 - billing reports, using Reporter
 - to monitor service usage 258
 - breaches, security
 - types 402
 - why they happen 405
 - broadening a user search 73
 - Building Block Summary report 468
 - monitoring outdialing services 452, 453
- ## C
- cabling, security guidelines 419
 - call authorization, how it works 488
 - call restrictions, implications 489
 - calling line ID. *See* CLID
 - CallPilot Administration Client
 - adding a system 51
 - grouping systems into a site 54
 - working with 51

- CallPilot Performance Monitor 457
 - CallPilot server tools 443
 - changing
 - Administrator password 425
 - administrator's access class 83
 - archive device 236
 - mailbox user 90
 - NGenDesign password 426
 - NGenDist password 426
 - NGenSys password 426–428
 - passwords 423–428, 429
 - pcANYWHERE32 password 429–430
 - SDL 136
 - user's administrative capability 83, 84
 - user's personal information 82
 - channel allocation
 - Outcalling services
 - maximums in SDN Table 381
 - minimums in SDN Table 380
 - channel state descriptions 381
 - channels
 - distribution 256
 - starting and stopping 255
 - state descriptions 255
 - states, how they are shown 255
 - what they do 255
 - checking
 - last mailbox access 101
 - number of invalid logon attempts 102
 - user's recorded greeting status 99
 - user's storage space 98
 - checklist, security 432
 - access classes 432
 - mailbox security 433–434
 - restriction/permission lists 432–433
 - choosing users for SDL 121
 - Class of Service 487
 - and TGAR 494
 - flowchart 496
 - how it works
 - with TGAR 495
 - recommendations for agents 497
 - clearing alarms 286
 - CLIDs
 - monitoring with Hacker Monitoring 464
 - alarms followup 465
 - external versus internal 464
 - generated alarms 465
 - logon attempts 464
 - thru-dials 464
 - when to do 464
 - removing from monitoring list 474
 - setting up monitoring for 473
 - client systems, security guidelines 419
 - CLS. *See* Class of Service
 - common user search examples 70
 - conditions, user search 67
 - corporate security guidelines
 - equipment 418
 - information 420
 - premises 417
 - creating
 - and maintaining SDLs 103
 - directory entry for SDL 131
 - remote user for SDL 126
 - creating an SDL
 - labeling the SDL 119
 - critical (event severity level) 262
 - customizing
 - event logs 275, 312
 - severity filters 275
 - using filters 275
- D**
- data, server performance
 - studying 338
 - viewing 339
 - database (disk space)
 - exceeded limits, causes and solutions 334
 - monitoring 250, 325
 - limits 334
 - default user accounts 423
 - defining
 - mailbox settings for a remote user 127
 - deleting
 - mailbox user 91
 - saved user search 80
 - user 91
 - Delivery to Fax
 - failure events 385

- failures 385
 - troubleshooting 383
- retry strategy after delivery failure 383
- why delivery failures happen 383
- Delivery to Telephone
 - failure events 385
 - failures 385
 - troubleshooting 383
 - retry strategy after delivery failure 383
 - why delivery failures happen 383
- desktop
 - locking 85
 - unlocking (restoring access) 87
- detecting
 - hardware problems 253
 - system problems 258
- deterioration of service, investigating 457
- diagnostic tools, accessing 31
- diagram, how messages are sent to a distribution list 109
- dialing privileges, agents 498
 - implications 498, 498–499
- dialing restrictions, applying to CallPilot
 - features 437
- directory entry
 - defining settings for 132
- disabled mailbox 94
- Disk Administrator
 - accessing 31
- disk partitions 324
- disk space
 - monitoring 249, 324
 - database 250, 325
 - Disk Usage window 330
 - MMFS volumes 250, 325, 327
 - Nortel directory 249, 324, 326
 - Reporter 330
 - Server Performance Monitor 330
 - usage 250
 - nightly audit 325
 - reducing used space 330
 - message retention 330
 - OM retention 331
 - storage 331
 - why you should monitor 249, 324
- Disk Usage window 330

- distributing channels 256
- distribution list
 - definition 108
 - how messages are sent to 109

E

- efficiency, evaluating system 258
- enhancements, types of user 63
- establishing baseline using Reports 257, 442
- evaluating system efficiency 258
- Event Browser 246, 247, 264, 266, 290, 456
 - accessing the window 273, 311
 - critical events 272
 - description 272
 - event codes 263
 - event type 273
 - filtering events 275
 - purpose 272
 - subset of all events 277
 - viewing event codes 274
- event codes 263
 - override default parameters 292
- event logs
 - definition 266
 - filters for 275, 312
 - impact of changes 266
 - saving and printing 278
 - severity filters 275
 - size 266
 - changing 266
 - default 267
- event preference
 - changing 295
 - creating 293
 - deleting 296
- Event Preferences 246
 - accessing the window 293
 - the program 292
 - working with 247
- event severity levels
 - critical 262
 - information 263
 - major 262
 - minor 262

- event types
 - clear 262
 - information 262
 - set 262
- Event Viewer, accessing 31
- event, definition of an 246
- events
 - filtering 247
 - filtering versus throttling 247
 - Outcalling failures 385
 - printing 312
 - printing all 275
 - processing, hardware problems 253
 - Remote Notification failures 386
 - Remote Notification server failures 386
 - severity 246
 - throttling 247, 290
 - working with 246
 - Event Browser 247
 - Event Preferences 246
- excessive
 - after-hours logon attempts 449
 - what to do 449
 - incomplete messaging accesses alert 448
 - what to do 448
 - thru-dialer accesses 449
 - what to do 449
- existing user search
 - deleting a saved search 80
 - re-using the last search 77
 - using a saved search 79
- external logon and hacker attacks 439

F

- Facility Restriction Levels 490
- fault management, definition 253
- fax callback, hacker use 409
- features, CallPilot security 410, 484
- filtering events 247
 - versus throttling 247
- filters
 - for event logs 275, 312
 - settings 275
 - severity 275

- flowcharts
 - TGAR and CLS 496
- fraud, toll
 - protecting system 408
 - susceptible services 484
- frequency, archive 215
- frequently performed tasks 93
- FRLs. *See* Facility Restriction Levels

G

- generating reports 389
- greeting
 - status, viewing mailbox 99
 - verifying 99
- greetings
 - hacker pranks 408
 - protecting 412

H

- Hacker Monitoring 413, 444
 - alarm notification 462
 - Application Builder services monitoring 468
 - alarms followup 469
 - Building Block Summary report 468
 - generated alarms 468
 - CLID monitoring 464
 - alarms followup 465
 - external versus internal 464
 - generated alarms 465
 - logon attempts 464
 - thru-dials 464
 - when to do 464
 - definition 462
 - mailbox monitoring 466
 - alarms followup 467
 - generated alarms 466
 - logon attempts 466
 - thru-dials 466
 - what you can monitor 462
 - when to use 462
- hacker techniques
 - external logon use 439

- fax callback use 409
- getting information 406
- logging on 406
- mailbox use 408
- message and greeting pranks 408
- modem use 501
 - eliminating 501
- hardware problems
 - alarms notification 253
 - detecting 253
 - event processing 253
 - fault management, definition 253
 - isolating 254
- Help
 - online 23, 274

I

- Inactive User report 451
 - what to do 451
- increasing mailbox storage 96
- information
 - printed, security guidelines 420
 - protecting from hackers 406
 - types of user 61
 - administrative capabilities 62
 - general 62
 - mailbox capabilities 62
- information (event severity level) 263
- invalid logon attempts, limiting 439
- invalid mailbox logon attempts, viewing 102
- IP address 52
 - changing 394
- isolating hardware problems 254

L

- LAN, protecting from security threats 412
- layers of security 404
 - types 485
- legal responsibility, in regards to security 403
- limitations on starting and stopping call channels 346
- limiting a user search 75
- list name for an SDL 120

- local users
 - adding to an SDL 125
- locking out other administrators 85
- logging on to Windows NT 29
- logging on, hacker techniques 406
- logon
 - attempts, limiting invalid 439
 - disabling external 439
 - viewing invalid mailbox 102

M

- mailbox
 - alarm 479
 - setting up 479
 - setting up immediate notification 479, 480
 - deleting 91
 - hacker use of 408
 - logon attempts, checking invalid 102
 - managing 90
 - monitoring with Hacker Monitoring 466
 - alarms followup 467
 - generated alarms 466
 - logon attempts 466
 - thru-dials 466
 - password, resetting 95
 - printing 92
 - protecting 411
 - reenabling 94
 - removing from monitoring list 476
 - securing passwords 439
 - setting up monitoring for 475
 - storage, increasing 96
- Mailbox Call Session Summary report 451
 - what to do 451
- mailbox user
 - Autologon
 - disabling 97
 - enabling 97
 - changing 90
 - deleting 91
 - greeting, viewing status 99
 - invalid logon attempts, viewing 102
 - last access, viewing 101
 - password, resetting 95

- printing
 - detailed information 92
 - from Users list 92
- reenabling 94
- status, viewing 98
- storage, increasing 96
- maintenance, user, activities 60
- major (event severity level) 262
- Management Information Base 302
- managing
 - users 55
 - users' mailboxes 90
- managing call channels 343
 - call channels and their states 347
 - starting call channels 355
 - stopping call channels 357
 - viewing call channel states 352
- managing multimedia channels
 - channel states 364
 - disabled channels 366
 - media types 363
- MAT Alarm Notification tool 302
- Meridian Mail Trunk Access Restriction
 - definition 500
 - why use it 500
- message delivery failures
 - retry strategy 383
 - why they happen 383
- message length for SDLs 113
- message size for SDLs 112
- messages, hacker pranks 408
- messaging system, how hackers log on 406
- methods to stop a channel
 - courtesy stop 357
 - stop 357
- MIB. *See* Management Information Base
- minor (event severity level) 262
- MMFS volumes
 - alarms 328
 - clearing 328
 - monitoring disk space 250, 325, 327
- modems
 - eliminating hacker risk 501
- monitoring
 - Application Builder services
 - removing from monitoring list 478
 - setting up 477
- CLIDs
 - removing from list 474
 - setting up 473
- database (disk space) 250
 - limits 334
- disk space 249, 324
 - database 325
 - Disk Usage window 330
 - MMFS volumes 325, 327
 - Nortel directory 324, 326
 - Reporter 330
 - Server Performance Monitor 330
- disk usage 250
- exceeded database (disk space) limits, causes
 - and solutions 334
- mailbox
 - removing from list 476
 - setting up 475
- MMFS volumes 250
- Nortel directory 249
- server performance 252
- system
 - for security reasons 412
 - security 258
- tools 17, 442
 - CallPilot 443
 - Hacker Monitoring 444
 - Reporter 443
 - Windows NT Server 443
- with Hacker Monitoring 462
- MTAR. *See* Meridian Mail Trunk Access Restriction
- multimedia channels
 - available number 361
 - Multimedia Monitor window 362
 - powering multimedia channels on and off 371
 - starting 373
 - stopping 375
 - viewing multimedia channel media types 370
 - viewing multimedia channel states 367
- multimedia messages
 - and SDLs 113

N

- narrowing user search 75
- NCOS. *See* Network Class of Service
- Network Class of Service 487
 - agent recommendations 493
 - definition 490
- Network Management System 298
- Network Management System (NMS) 299, 302
- networking requirements for SDLs 111
- NGenDesign account
 - changing password for 426
- NGenDist account
 - changing password for 426
- NGenSys account
 - changing password for 426–428
- nightly audit, disk space 325
- NMS. *See* Network Management System
- Nortel directory
 - alarms 326
 - monitoring disk space 249, 324, 326
- Nortel SMI window
 - locking 85
 - restoring access 87
- notification, alarms
 - hardware problems 253
 - setting up 479, 480
- number of available multimedia channels 361
- number of messages for SDLs 112

O

- online Help 23, 274
 - event codes 283
- opening an SDL 116
- Operational Measurements
 - and Reporter 46
 - Billing OMs 44
 - collecting OM data 47
 - collecting/storing OM data 43
 - data storage 47
 - how to use 43
 - OM data storage duration 43
 - programs and tools that use 41
 - Trace OMs 45

- Traffic OMs 44
 - types of OM data 44
- Operator, user search 69
- Outcalling problems
 - types of 380
 - cannot place call 380
 - DTF failures 383
 - DTT failures 383
 - Remote Notification failures 384
 - using reports to troubleshoot 388
- Outcalling services
 - protecting 411
 - SDN Table, maximum channel allocations 381
 - SDN Table, minimum channel allocations 380

P

- partitions, disk 324
- password blocks, checking for Application Builder services alarms 469
- passwords
 - guidelines for 424
 - maintaining 423–428, 429
 - resetting a user mailbox password 95
 - resetting for administrator 89
 - securing mailbox 439
- pcANYWHERE32 password, changing 429–430
- PDL
 - definition 110
 - number of entries per address 112
 - restrictions 110
- performance data, server
 - studying 338
 - viewing 339
- Performance Monitor
 - CallPilot, using to investigate service deterioration 457
 - Windows NT 458
- performance, server
 - monitoring 252
 - why you should monitor 252
- performing an immediate archive 231
- personal distribution list. *See* PDL
- placeholder, user search 69

- policy, security 404
- preventing, administrator access 85
- printing
 - all alarms 309
 - all events 275
 - all Server Performance Monitor data 341
 - contents of an SDL 139
 - mailbox user
 - detailed information 92
 - from Users list 92
 - SDLs 139
 - selected Server Performance Monitor data 341
- privileges, agent dialing 498
 - implications 498, 498–499
- problems, Outcalling
 - types of 380
 - cannot place call 380
 - DTF failures 383
 - DTT failures 383
 - Remote Notification failures 384
 - using reports to troubleshoot 388
- prompt archive 216, 217
- prompts
 - protecting 412
 - restoring prompts 241
- protecting
 - corporate information from hackers 406
 - from toll fraud 408
 - system from hackers 406

R

- recommendations for agents
 - CLS 497
 - NCOS 493
- reenabling a mailbox 94
- remote logon 429
- Remote Notification
 - failure events 385, 386
 - server failure events 386
 - setting up for alarm mailbox 480
 - troubleshooting failures 384
- remote users
 - adding to an SDL 130

- removing
 - applications from an Application Builder archive 223
 - user's administrative capability 84
 - users from a user archive 227
- Reporter
 - and OM data 46
 - description 443
 - Outcalling troubleshooting 388
 - why use 257
- reports
 - Building Block Summary, monitoring outdialing services 452, 453
 - generating 389
 - Inactive User
 - what to do 451
 - Mailbox Call Session Summary
 - what to do 451
 - System Traffic Summary, monitoring Call Answering 452
 - using event logs 275, 312
 - Voice Messaging Activity, detecting hacker activity 452
- requests, types of user 63
- resetting
 - administrator password 89
 - user password 95
- Restore Manager, description 217
- restoring
 - administrator access 87
 - Application Builder applications from an archive 237
 - latest user search 77
 - prompts 241
 - user data 239
 - user data from archive 239
- restricting
 - a user search 75
 - administrator access 435
- restriction/permission lists 487
 - applying to CallPilot services 438
 - checking for Application builder services alarms 469
 - creating 437
- restrictions
 - agents 485

- CallPilot and Meridian 1 features 487
 - dialing privileges 487
- dialing, applying 437
- implication for calls and agents 489
- on distribution list numbers 112
- on PDLs 110
- on SDLs 112
- retrieving a user search 77
- risks, understanding security 404
- RPLs. *See* restriction/permission lists
- running a saved user search 79

S

- saving a user search 78
- schedule
 - performing an immediate archive 231
 - setting up a schedule for an archive 229
- screen descriptions, Server Performance Monitor 339
- screen examples
 - Search Users dialog 68
 - Security Administration 472
 - Server Performance Monitor 339
 - Switch Resources 319
 - Users 61
- SDL
 - adding a single user 123
 - adding all users 124
 - adding local users 125
 - adding remote users 130
 - and multimedia messages 113
 - changing 136
 - creating and labeling 119
 - creating user list for 122
 - defining a remote user's settings 127
 - defining the settings for a directory entry 132
 - definition 110
 - delete a user 137
 - delete an SDL 138
 - guidelines for creating 112
 - identifying a directory entry with a WAV file 134
 - message length 113
 - number of addresses 113

- number of entries per address 112
- number of messages and message size 112
- opening 116
- printing 139
- printing contents 139
- recording a list name 120
- requirements for networking 111
- restrictions 112
- setting up 117
- types of user entries 111
- viewing 135
- what users can be included 111

- SDN Table 381
 - Outcalling services
 - maximum channel allocations 381
 - minimum channel allocations 380
- Search Criteria, field description 68
- search for users, overview 66
- Search Users dialog, screen example 68
- searching for users 65
 - common search examples 70
 - conditions 67
 - deleting a saved search 80
 - description 67
 - for a user archive 227
 - how it is done 66
 - narrowing search 75
 - Operator field 69
 - performing search 71
 - re-using the last search 77
 - saving 78
 - tip 71
 - to add to SDL 122
 - using a saved search 79
 - Value field 68
 - when to do 66
 - widening search 73
- security
 - administrator accounts 410
 - agent restrictions 485
 - CallPilot and Meridian 1 features 487
 - dialing privileges 487
 - breaches
 - type 402
 - why they happen 405
 - cabling and wiring guidelines 419

- CallPilot features 410, 484
- checklist 432
 - access classes 432
 - mailbox security 433–434
 - restriction/permission lists 432–433
- client machine guidelines 419
- equipment room guidelines 418
- Hacker Monitoring 413
- layers 404, 485
- legal responsibility 403
- log 263
- modems 501
 - reducing risk 501
- policy 404
- premises guidelines 417
- printed information guidelines 420
- protection
 - greetings and prompts 412
 - LAN 412
 - mailbox 411
 - outcalling services 411
- system, monitoring with Reporter 258, 412
- threats 402
- understanding risks 404
- Windows NT Performance Monitor 458
- workstation guidelines 419
- security alerts
 - excessive after-hours logon attempts 449
 - what to do 449
 - excessive incomplete messaging accesses 448
 - what to do 448
 - excessive thru-dialer accesses 449
 - what to do 449
- security reports
 - Building Block Summary, monitoring
 - outdialing services 452, 453
 - Inactive User 451
 - what to do 451
 - Mailbox Call Session Summary 451
 - what to do 451
 - System Traffic Summary, monitoring Call Answering 452
 - Voice Messaging Activity, detecting hacker activity 452
- selecting the languages of prompts to be restored 241
- Server Manager, accessing 31
- server performance
 - data, studying 338
 - data, viewing 339
 - monitoring 252
 - why you should monitor 252
- Server Performance Monitor 330
 - accessing 31
 - printing all data 341
 - printing selected data 341
 - screen description 339
 - screen example 339
 - technical support, when to contact 340
 - CPU usage 340
 - free disk space 340
 - memory usage 340
- server, user accounts on 423
- service deterioration, investigating 457
- services
 - applying restriction/permission lists 438
 - monitoring usage with Reporter 258
 - Outcalling 381
 - Outcalling, protecting 411
 - susceptible to toll fraud 484
- setting up
 - access classes 435
 - Application Builder archive 221
 - customized prompts archive 228
 - schedule for an archive 229
 - SDL 117
 - user archive 224
- severity levels
 - critical 262
 - information 263
 - major 262
 - minor 262
- severity, event 246
- shared distribution list. *See* SDL
- shutting down system
 - from Windows NT 32
- Simple Network Management Protocol 298, 299
- SNMP. *See* Simple Network Management Protocol
- space, disk
 - monitoring 249, 324

- database 250, 325
- Disk Usage window 330
- MMFS volumes 250, 325, 327
- Nortel directory 249, 324, 326
- Reporter 330
- Server Performance Monitor 330
- usage 250
- nightly audit 325
- reducing used space 330
 - message retention 330
 - OM retention 331
 - storage 331
- why you should monitor 249, 324
- specifying search criteria 71
- speed of backup 147
- starting channels 255
- starting multimedia channels 373
- states
 - channel, description 255, 381
 - how they are shown for channels 255
- status
 - checking user 64
 - viewing mailbox 98
- stopping channels 255
- stopping multimedia channels 375
- storage space
 - increasing for mailbox 96
 - verifying 98
- suspicious activity, tracking with Hacker Monitoring 413
- switch configuration 318
- Switch Resources, screen example 319
- system
 - adding to CallPilot 51
 - behavior
 - establishing a baseline using Reports 257, 442
 - patterns 442
 - computer name 52
 - efficiency, evaluating 258
 - grouping systems into a site 54
 - IP address 52
 - monitoring for security reasons 412
 - monitoring tools 442
 - CallPilot 443
 - Hacker Monitoring 444

- Reporter 443
- Windows NT Server 443
- network connection 51
- on the CallPilot Administration Explorer tree 53
- problems, detecting with Reporter 258
- security
 - guidelines 418
 - monitoring with Reporter 258
- system name 53
- system date and time, viewing the 37
- system shutdown from Windows NT 32
- System Traffic Summary report 452
- monitoring Call Answering 452

T

- technical support, when to contact 340
 - CPU usage 340
 - free disk space 340
 - memory usage 340
- TGARs. *See* Trunk Group Access Restriction
- threats, security 402
- throttling events 247
 - versus filtering 247
- thru-dialer accesses 449
 - what to do 449
- toll fraud
 - fax callback use by hackers 409
 - how to prevent 408
 - susceptible services 484
- Trace OMs 45
- tracking suspicious activity, Hacker Monitoring 413
- Traffic OMs 44
- troubleshooting
 - CallPilot is improperly configured 393
 - calls answered but no prompts heard 393, 396, 397
 - calls not answered 393, 396
 - examples 396
 - Outcalling
 - cannot place call 380
 - DTF failures 383
 - DTT failures 383

- Remote Notification failures 384
 - using reports 388
- switch is improperly configured 393
- system is not working after a change in IP address 394
- system monitor shows a blue screen 393
- system not working after a change in IP address 394
- Trunk Group Access Restriction 487
 - agent recommendation 494
 - and CLS
 - flowchart 496
 - how it works 494
 - with CLS 495
 - their role in CallPilot security 493
- types of archives 216
 - Application Builder 216
 - prompt 217
 - user 216

U

- unsuccessful logon attempts 448
 - what to do 448
- usage
 - disk, monitoring 250
 - service, monitoring 258
- used space, reducing on disk 330
 - message retention 330
 - OM retention 331
 - storage 331
- user
 - accounts on server 423
 - administrative
 - locking out 85
 - resetting password 89
 - restoring access 87
 - administrative access
 - adding 83
 - changing 84
 - removing 84
 - archive 216
 - Autologon
 - disabling 97
 - enabling 97
 - common changes example 62
 - data, restoring from archive 239
 - delete from an SDL 137
 - deleting 91
 - enhancements, types of 63
 - frequent requests 63
 - how to maintain the users on your system 60
 - information
 - administrative capabilities 62
 - general 62
 - mailbox capabilities 62
 - personal, changing 82
 - types of 61
 - mailbox
 - access, viewing 101
 - changing 90
 - deleting 91
 - greeting, viewing status 99
 - invalid logon attempts, viewing 102
 - managing 90
 - printing 92
 - reenabling 94
 - status, viewing 98
 - storage, increasing 96
 - maintenance activities 60
 - password, resetting 95
 - printing 92
 - detailed information 92
 - from Users list 92
 - requests, types of 63
 - search
 - common examples 70
 - conditions 67
 - deleting 80
 - deleting a saved search 80
 - description 67
 - how it is done 66
 - narrowing 75
 - Operator field 69
 - performing 71
 - restoring 77
 - re-using the last search 77
 - running an existing 79
 - saving 78
 - tip 71
 - using a saved search 79

- Value field 68
 - when to perform 66
 - widening search 73
- searching for users 65
- status, checking 64
- User Manager
 - accessing 31
- User Profile Editor
 - accessing 31
- Users, screen example 61
- using Reporter, troubleshooting Outcalling problems 388

V

- value, user search 68
- view the system date and time 37
- viewing
 - invalid mailbox logon attempts 102
 - last mailbox access 101
 - mailbox greeting status 99
 - mailbox status 98
 - SDL 135
 - system date and time 37
- Voice Messaging Activity report 452
 - detecting hacker activity 452

W

- warning signals, alerts 446
- when to stop channels 358
- widening user search 73
- wildcards, user search 68
- Windows NT 299
 - access diagnostic tools 31
 - default settings for event log 267
 - Event Viewer 263
 - logging on to 29
 - Performance Monitor 458
 - Server tools 443
- Windows NT Event Viewer 290
- wiring, security guidelines 419
- workstations, security guidelines 419

CallPilot

Monitoring and Security for the Administrator

Toronto Information Products
Nortel Networks
522 University Avenue, 14th Floor
Toronto, Ontario, Canada
M5G 1W7

Copyright © 2000 Nortel Networks, All Rights Reserved

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

The process of transmitting data and call messaging between the Meridian 1 and CallPilot is proprietary to Nortel Networks. Any other use of the data and the transmission process is a violation of the user license unless specifically authorized in writing by Nortel Networks prior to such use. Violations of the license by alternative usage of any portion of this process or the related hardware constitutes grounds for an immediate termination of the license and Nortel Networks reserves the right to seek all allowable remedies for such breach.

Publication number:	555-7101-307
Product release:	1.07
Document release:	Standard 1.0
Date:	April 2000

Printed in the United States of America

*Nortel Networks, the Nortel Networks logo, the Globemark, How the World Shares Ideas, and Unified Networks, BNR, CallPilot, DMS, DMS-100, DMS-250, DMS-MTX, DMS-SCP, DPN, Dualmode, Helmsman, IVR, MAP, Meridian, Meridian 1, Meridian Link, Meridian Mail, Norstar, SL-1, SL-100, Supernode, Symposium, Telesis, and Unity are trademarks of Nortel Networks.

MICROSOFT, MS-DOS, POWERPOINT, WINDOWS, and WINDOWS NT are trademarks of Microsoft Corporation.

PCANYWHERE is a trademark of Symantec Corporation.

SLR4, SLR5, and TANDBERG are trademarks of Tandberg Data ASA.



How the world shares ideas.